



NOT MEASUREMENT
SENSITIVE

National Aeronautics and
Space Administration

NASA-STD-8729.1
December 1998

PLANNING, DEVELOPING AND
MANAGING AN EFFECTIVE
RELIABILITY AND MAINTAINABILITY
(R&M) PROGRAM

NASA TECHNICAL STANDARD

FOREWORD

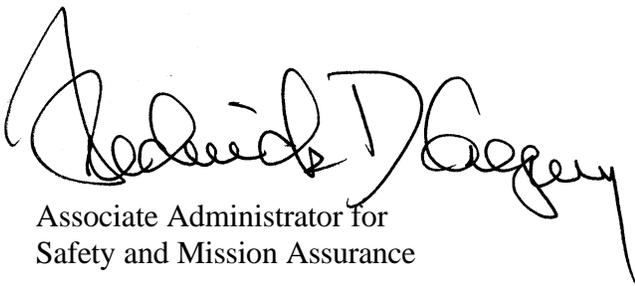
This NASA Technical Standard provides a centralized source of information for promoting Reliability and Maintainability (R&M) concepts and operational requirements on all new NASA programs. In addition these concepts should be considered for application to existing programs/projects where their application is cost effective. The objective of this R&M Technical Standard is to establish and maintain a high level of R&M managerial and technical excellence throughout NASA and its suppliers/ contractors.

The Standard contains a broad, tailorable approach for implementing R&M techniques that emphasize R&M performance requirements for assured mission success. It reflects both the new system acquisition phasing and the change from government “oversight” to “insight” described in NASA NPG 7120.5A as well as the R&M programmatic policy of NPD 8720.1. It consists of specific management and technical actions designed to ensure successful system operations in the rapidly changing space and aeronautics environment.

It provides guidance for development and application of R&M early in the acquisition process, integration of R&M within the systems engineering process, and evaluation of R&M performance progress in both new and, as appropriate, existing programs/projects. Tailorable R&M requirements language is also provided for use in structuring statements of work for procurements. NASA should use this document in planning requirements for R&M in procurements, in-house hardware/software development efforts, and existing programs/projects.

Early application of the concepts and principles in this document will aid the program/project manager in reducing or eliminating risks to mission success at a point where the costs of such efforts are at their minimum. Application to mature programs/projects will assure rigorous treatment and resolution of problems that arise during operations.

General questions on the intent of this R&M Technical Standard should be referred to the National Aeronautics and Space Administration Headquarters, Director, Safety and Risk Management Division (Code QS), Washington, DC 20546-0001. Questions concerning the application of these R&M concepts to specific NASA programs/projects should be referred to the cognizant NASA Directors. Copies of this publication are available from the World-Wide-Web at <http://www.hq.nasa.gov/office/codeq/qdoc.pdf>.



Associate Administrator for
Safety and Mission Assurance

NASA TECHNICAL STANDARDS FOR SAFETY AND MISSION ASSURANCE

NASA Technical Standards can be found on the World Wide Web at URL address

<http://www.hq.nasa.gov/office/codeq/qdoc.pdf>

Title	Number
Facilities System Safety Guidebook	NASA-STD-8719.7
ELV Payload Safety Review Process	NASA-STD-8719.8
NASA Safety Standard for Lifting Devices and Equipment	NASA-STD-8719.9
NASA Safety Standard for Underwater Facility and Non-Open Water Operations	NASA-STD-8719.10
NASA Safety Standard for Fire Protection	NASA-STD-8719.11
NASA Safety Standard for Explosives, Propellants and Pyrotechnics	NASA-STD-8719.12
NASA Software Safety Standard	NASA-STD-8719.13
Safety Standard for Oxygen and Oxygen Systems	NASA-STD-8719.15
Safety Standard for Hydrogen and Hydrogen Systems	NASA-STD-8719.16
Soldered Electrical Connections	NASA-STD-8739.3
Crimping, Interconnecting Cable Harness and Wiring	NASA-STD-8739.4
Fiber Optic Terminations, Cable Assemblies, and Installation	NASA-STD-8739.5
Requirements for Conformal Coating and Staking	NASA-STD-8739.1
Requirements for Surface Mount Technology	NASA-STD-8739.2
Requirements for Electrostatic Discharge Control	NASA-STD-8739.7
Design Standard for Rigid Printed Boards and Rigid Printed Board Assemblies	IPC-D-275
Quality Performance Specification for Rigid Printed Wiring Boards	IPC-RB-6011& 6012
Procurement Specification for Rigid Printed Boards for Space Applications and Other High Reliability Uses	GSFC S-312-P003

CONTENTS

<u>PARAGRAPH</u>	<u>PAGE</u>
FOREWORD	i
NASA TECHNICAL STANDARDS FOR SAFETY AND MISSION ASSURANCE	ii
TABLE OF CONTENTS	iii
LIST OF FIGURES	v
LIST OF TABLES	v
LIST OF APPENDICES	v
1. SCOPE	1-1
1.1 Purpose	1-1
1.2 Applicability	1-1
1.3 Approval of Departures from this Standard	1-2
2. APPLICABLE DOCUMENTS	2-1
2.1 Applicable Documents	2-1
2.2 Other Documents	2-1
3. DEFINITIONS AND ACRONYMS	3-1
3.1 Definitions	3-1
3.2 Acronyms	3-11
4. GENERAL	4-1
4.1 NASA R&M Policy	4-1
4.2 R&M Approach	4-1
4.3 R&M Customer	4-3
4.4 R&M Training	4-4
5. R&M OVERVIEW	5-1
5.1 R&M and the Acquisition Process	5-1
5.1.1 Formulation	5-1
5.1.2 Approval	5-3
5.1.3 Implementation	5-3
5.1.4 Evaluation	5-3
5.2 R&M Integration with Other Organizational Elements	5-4
5.2.1 Manufacturing and Quality Assurance	5-4
5.2.2 Human Engineering	5-5
5.2.3 Safety	5-5
5.2.4 Diagnostics and Maintenance	5-5
5.2.5 Logistics Support	5-5
5.2.6 Software	5-6
5.2.7 Program/Project Engineering	5-6

CONTENTS – CONT.

5.3	Acquisition Initiatives Related to R&M	5-6
5.3.1	Performance-Based Contracting	5-6
5.3.2	Risk Management.....	5-7
5.3.3	Metrics.....	5-7
5.3.4	Single Process Initiative	5-8
5.4	Summation.....	5-8
6.	R&M IN FORMULATION	6-1
6.1	Goal of Formulation	6-1
6.2	Program Management Activities Related to R&M	6-1
6.2.1	Developing of the Acquisition Strategy	6-1
6.2.2	Developing the Acquisition Team.....	6-1
6.2.3	Exploring Implementation Options	6-2
6.2.4	Developing Program/Project Metrics and Performance Assessment Criteria.....	6-2
6.2.5	Performing Life Cycle Costing	6-3
6.2.6	Developing the Operations Concept	6-4
6.2.7	Developing a Fault Detection, Isolation and Recovery (FDIR) Capability	6-5
6.3	Risk Management Activities Related to R&M	6-5
6.3.1	Preparing the Risk Management Plan (RMP).....	6-5
6.3.2	Establishing Mission Success Criteria	6-5
6.3.3	Preliminary Risk Identification and Risk Mitigation Planning	6-6
6.3.4	Capturing Risk History and Lessons Learned.....	6-6
7.	R&M IN APPROVAL.....	7-1
7.1	Goal of Approval	7-1
7.2	Activities Related to R&M.....	7-1
8.	R&M IN IMPLEMENTATION	8-1
8.1	Goal of Implementation.....	8-1
8.2	Program/Project Management Activities Related to R&M.....	8-1
8.2.1	Requirements Definition.....	8-1
8.2.1.1	Conversion of Program/Project Requirements into Specifications	8-1
8.2.1.2	The Need for R&M Performance Requirements on NASA Programs/Projects ..	8-1
8.2.1.3	Defining R&M Performance Requirements.....	8-2
8.2.1.4	Establishing R&M Incentives	8-3
8.2.2	R&M Considerations in Systems Design.....	8-4
8.2.2.1	Typical/Example Considerations.....	8-4
8.2.2.2	Closed Loop Problem/Failure Reporting.....	8-5
8.2.3	Test and Verification.....	8-5
8.2.3.1	R&M Performance Requirements Verification.....	8-5
8.2.3.2	Test and Evaluation.....	8-6
8.2.3.3	R&M System/Product Acceptance	8-8
8.2.4	Operations and Logistics	8-8

CONTENTS – CONT.

8.2.4.1	R&M during Operations.....	8-8
8.2.4.2	Logistic Support	8-9
8.2.5	Risk Management Activities Related to R&M	8-10
8.2.6	R&M Program/Project Reviews	8-10
9.	R&M IN EVALUATION	9-1
9.1	Goal of Evaluation	9-1
9.2	Evaluation Subprocess Activities Related to R&M	9-1

FIGURES

<u>NUMBER</u>		<u>PAGE</u>
4-1	Generic R&M Process.....	4-2
5-1	R&M Program within the Acquisition Subprocesses.....	5-2

TABLES

<u>NUMBER</u>		<u>PAGE</u>
6-1	Typical Reliability, Maintainability, and Availability Parameters used to Quantify R&M Performance.....	6-4
8-1	Considerations in Design for R&M.....	8-4
8-2	R&M Trade-off Analysis Examples	8-4
8-3	Critical Maintainability Criteria.....	8-4
8-4	Typical R&M T&E Program/Project Process-Related Activities	8-7
8-5	Quantitative Reliability Requirements Verification Techniques.....	8-8
8-6	Typical Logistics Support Considerations.....	8-10

APPENDICES

Appendix A	R&M Toolsets	A-1
	Reliability Analysis Toolset	A-2
	Maintainability Analysis Toolset	A-7
	Reliability Test and Evaluation Toolset.....	A-9
	Maintainability Test and Evaluation Toolset	A-13
	Technical Review Toolset	A-14
Appendix B	Key R&M Discipline Definitions	B-1
Appendix C	Statement of Work - Reliability and Availability	C-1
Appendix D	Statement of Work - Maintainability.....	D-1

CHAPTER 1 - SCOPE

1.1 Purpose

This technical standard for reliability and maintainability (R&M) provides guidance to customers (or purchasers) and suppliers (or contractors) on R&M requirements development, design implementation, and evaluation. It has been developed to provide a centralized source of information for establishing R&M performance-based requirements, design factors, and metrics for use on all new NASA programs/projects and contracts. It addresses the challenge of managing mission risk in the development and operation of cost and time constrained flight programs/projects and other NASA assets.

This document is intended as a guide to current techniques to identify and meet customer product performance expectations. It is structured to reflect the requirements of NPG 7120.5A "NASA Program and Project Management Processes and Requirements" and the programmatic policy of NPD 8720.1 "NASA Reliability and Maintainability Program Policy" as they relate to the R&M disciplines in the Formulation, Approval, Implementation, and Evaluation subprocesses of NASA programs/projects. It replaces previous NASA handbooks which were derived from military standards and which mandated general reliability and maintainability requirements for NASA programs/projects. This movement away from rigid standards and toward flexible guidelines reflects government's increased willingness to accept mature, controlled commercial practices and seek industry solutions in the development of civil and military systems. This guidance is intended to assist engineering managers in achieving the following R&M objectives throughout the life cycle of NASA in-house and contracted activities:

- Provide realistic R&M requirements for system development specifications and requirements documents.
- Allow for early and continuing attention to R&M principles during system design.
- Achieve system reliability and maintainability as defined by the mission objectives.
- Control system life cycle cost by addressing operations and maintenance support cost drivers during system design.
- Measure, report and assess R&M performance throughout the system life cycle.
- Maintain a comprehensive and readily accessible database of success and failure data for use in prediction, problem trending, and assessment of progress toward system success goals throughout the system's life cycle as well as for establishment of R&M performance requirements for follow-on or new programs/projects.
- Emphasize continuous R&M improvement in each successive generation of the system and its elements.

1.2 Applicability

This standard is not intended to be applied on contracts, rather it provides information to assist NASA enterprises, industry partners, and contractors in interpreting and complying with NASA R&M policy. It also serves as a reference tool for coordinating efforts to achieve the quantitative reliability and maintainability performance defined for a mission.

While there have been significant changes in the traditional acquisition phases, integration of associated disciplines, and emphasis on better-faster-cheaper, it is still of the utmost importance to institute a strong and comprehensive reliability and maintainability program early in the acquisition process. In the old 5-phase acquisition process, delaying establishment of such a program was estimated to cost the program/project an order of magnitude per acquisition phase in effort and cost of redesign/rework to correct problems. Now that the old process has been converted into a 4-subprocess acquisition system, one might deduce that early application of R&M disciplines would have even greater benefits.

It is also noted that while maximum benefit is derived from early application of the R&M disciplines, benefits such as reduced operating cost and improved probability of success often can be realized with application later in a program/project or to existing programs/projects.

1.3 Approval of Departures from this Standard

This standard provides guidance and is not intended for use as a mandatory requirement; therefore, there is no approval required for departing from this standard. However, the fundamental principles related to designing-in R&M, as described in this standard, are considered an integral part of the systems engineering process and the ultimate R&M performance of the program/project is subject to assessment during each of the program/project subprocesses (Formulation, Approval, Implementation, and Evaluation).

CHAPTER 2 - APPLICABLE DOCUMENTS

2.1 APPLICABLE DOCUMENTS¹

(NASA) NPD 8720.1, NASA Reliability and Maintainability (R&M) Program Policy

(NASA) NPD 7120.4A, Program/Project Management

(NASA) NPG 7120.5A, NASA Program and Project Management Processes and Requirements

2.2 OTHER DOCUMENTS

(NASA) "NASA Systems Engineering Process for Programs and Projects," JSC 49040, Version 1.0, October 1994.

(NASA) Technical Memorandum 4322A "NASA Reliability Preferred Practices for Design and Test," Web Page: (<http://www.hq.nasa.gov/office/codeq/overvu.htm>)

(NASA) Technical Memorandum 4628A, "Recommended Techniques for Effective Maintainability," Web Page: (<http://www.hq.nasa.gov/office/codeq/mtechniq.htm>)

(NASA) "Reliability Centered Maintenance Guide for Facilities and Collateral Equipment," Web Page: (<http://www.hq.nasa.gov/office/codej/codejx/rcm.htm>), December 1996

"Reliability, Maintainability, and Supportability Guidebook: Third Edition," Society of Automotive Engineers International Reliability, Maintainability and Supportability Committee (G-11).

"Blueprints for Product Reliability," Reliability Analysis Center, Rome, NY, 1996

Ebeling, Charles E., "Introduction to Reliability and Maintainability Engineering," McGraw Hill, Inc. New York, 1997

Ireson, W. Grant (Editor), Coombs, Clyde F. (Contributor), et.al. "Handbook of Reliability Engineering and Management, 2nd Edition," McGraw Hill, Inc. New York, 1996

Nowlan, F. Stanley, and Heap, Howard F., "Reliability-Centered Maintenance," Office of Assistant Secretary of Defense (Manpower, Reserve Affairs and Logistics), Washington, DC , December 29, 1978

Smith, Anthony M, P.E., "Reliability-Centered Maintenance," McGraw Hill, Inc., New York, 1993

¹ Applicable Documents available at : <http://www.hq.nasa.gov/office/codeq/qdoc.pdf>

CHAPTER 3 - DEFINITIONS AND ACRONYMS

3.1 DEFINITIONS

Accessibility - A feature of hardware design layout and installation for ease and rapidity of admission (to perform visual inspection and maintenance) without introduction of fault or failure to the accessed hardware.

Allocation - The assignment of reliability (or maintainability) performance requirements to subsystems and elements within a system which will result in meeting the overall reliability (or maintainability) performance requirements for the system if each of these performance requirements is attained.

Architecture - A structure that shows the elements and their relationship for a set of requirements or a system concept or both.

Assembly - A hardware item composed of any number of parts or subassemblies, joined together to perform a specific function, which can be disassembled without destruction.

Assessment - An evaluation or appraisal of the state of a system, program/project or a portion of a program/project.

Availability - The probability that an item will be in an operable and committable state at the start of a mission when the mission is called for at a random time. Availability is generally defined as uptime divided by downtime; the specific definitions are provided below and diagrammed in the subsequent chart:

Availability, Inherent (A_i) - The probability that an item will operate satisfactorily at a given point in time when used under stated conditions in an ideal support environment. It excludes logistics time, waiting or administrative downtime, and preventive maintenance downtime. It includes corrective maintenance downtime. Inherent availability is generally derived from analysis of an engineering design and is calculated as the mean time between failure (MTBF) divided by the mean time between failure plus the mean time to repair (MTTR). It is based on quantities under control of the designer.

Availability, Achieved - The probability that an item will operate satisfactorily at a given point in time when used under stated conditions in an ideal support environment (i.e., that personnel, tools, spares, etc. are instantaneously available). It excludes logistics time and waiting or administrative downtime. It includes active preventive and corrective maintenance downtime.

Availability, Operational (A_o) - The probability that an item will operate satisfactorily at a given point in time when used in an actual or realistic operating and support environment. It includes logistics time, ready time, and waiting or administrative downtime, and both preventive and corrective maintenance downtime. This value is equal to the mean time between failure (MTBF) divided by the mean time between failure plus the mean downtime (MDT). This measure extends the definition of availability to elements controlled by the logisticians and mission planners such as quantity and proximity of spares to the hardware item.

Availability	MTBF	Active Corrective Maintenance	Preventive Maintenance	Logistics Downtime	Administrative Downtime
Inherent	X	X			
Achieved	X	X	X		
Operational	X	X	X	X	X

Baseline - *noun*: Document(s) or databases(s) that record a set of requirements or product solutions that can be changed only by formal, documented procedures. *verb*: To formally approve a baseline.

Built-In Test (BIT) - A test approach using self test hardware or software to test all or part of an equipment item or system. BIT denotes any self-test feature incorporated into a design for the purpose of detecting, diagnosing and isolating failures.

Compatibility - The capability of two or more items to exist or function in the same system or environment without mutual interference.

Component - An assembly or any combination of parts, subassemblies, assemblies mounted together, such as a transmitter or cryogenic pump.

Constraints - Boundaries limiting design freedom which can be defined by environmental factors, contractual requirements, internal program/project requirements, or other factors. Environmental factors may include operating temperatures, pressure, levels of dust, etc. Contractual and internal design constraints may include interfaces, reliability, maintainability, human factors, logistics support, physical mass and dimensions, standardization, costs, design and fabrication practices, personnel resource and training.

Contract - An agreement between two or more parties which is normally written and enforceable by law.

Contractor - A party under contract to provide a product or service at a specified cost to another party (or parties) to the contract, also known as the customer(s).

Critical Item List - A list of items which, because of special engineering or logistic considerations, requires an approved specification to establish technical or inventory control at the component level.

Criticality (of a failure) -A measure of the severity of a failure in relation to mission performance, hazards to material or personnel, and maintenance cost. Programs/projects typically establish their own criticality definitions and classifications.

Customer - The recipient of a product or service provided by a supplier or contractor.

Degradation - A gradual impairment in ability to perform one or more functions.

Design Constraints - Boundaries limiting design freedom which can be defined by environmental factors, contractual requirements, internal program/project requirements, or other factors.

Environmental factors may include operating temperatures, pressure, levels of dust, etc. Contractual and internal design constraints may include interfaces, reliability, maintainability, human factors, logistics support, physical mass and dimensions, standardization, costs, design and fabrication practices, personnel resource and training

Design Specification - Generic designation for a specification which describes functional and physical requirements for an article, usually at the component level of assembly or higher. In its initial form, the design specification is a statement of functional requirements with only general coverage of physical and test requirements. In many programs/projects the end item specifications supplant design specifications for the contract end-items; for articles not designated contractually as end-items, design specifications provide the basis for technical and engineering management control.

Diagnostics - Tools, procedures, or software coding used to either identify and troubleshoot system faults or to verify the integrity of a system.

Downtime - The total time a system is in a non-operable state. Total downtime is typically from supply, access, diagnosis, maintenance, replacement or repair, and verification/alignment.

End Item - The final production product when assembled or completed and ready for use.

Environment - The natural and induced conditions experienced by a system including its people, processes, and products during operational use, stand-by, maintenance, transportation, and storage.

Environmental Requirements - The expected worst case impact of the environment on the system or item as well as the allowed impact of the system or items on the environment.

Failure - An incident in which an item does not perform an intended function.

Failure Analysis - The conduct of electrical, chemical, or metallurgical evaluations to determine the specific cause of device failure.

Failure Mechanism - The process (e.g., physical, chemical, electrical, thermal) of degradation or the chain of events which results in a particular failure mode.

Failure Mode - The characteristic manner in which a failure occurs, independent of the reason for failure; the condition or state which is the end result of a particular failure mechanism; the consequence of the failure mechanism through which the failure occurs, i.e., short, open, fracture, excessive wear.

Failure Modes and Effects Analysis (FMEA) - Analysis of a system and the working interrelationships of its elements to determine ways in which failures can occur (failure modes) and the effects of each potential failure on the system element in which it occurs, on other system elements, and on the mission.

Failure Mode Effects and Criticality Analysis (FMECA) - Analysis of a system and the working interrelationships of its elements to determine ways in which failures can occur (failure modes) and the effects of each potential failure on the system element in which it occurs, on other system elements, and on the mission, and the study of the relative mission significance or criticality of all potential failure modes.

False Alarm - An indicated fault where no fault or failure exists.

Fault Isolation - The process of determining the approximate location of a fault.

Fault Tree Analysis - A deductive system reliability tool which provides both qualitative and quantitative measures of the probability of failure. It estimates the probability that a top level event will occur, systematically identifies all possible causes leading to the top event, and documents the analytic process to provide a baseline for future studies of alternative designs.

Hard-time – Process under which an item must be removed from service at or before a previously specified time.

Governing Program Management Council (GPMP) - Forums composed of NASA and/or Center Senior Management that assess program and project planning and implementation and provide oversight and direction as appropriate.

Hardware - Items made of a material substance but excluding computer software and technical documentation.

Human Error Risk Assessment - A process that identifies risks to designs, equipment, procedures, and tasks as a result of human error.

Human Factors - A body of information about human abilities, human limitations, and other human characteristics from a physical and psychological perspective that are relevant to the design, operations, and maintenance of complex systems.

Human Factors Engineering - The application of human factors information to the design of tools, machines, systems, tasks, jobs, and environments for safe, comfortable, and effective human use.

Human Factors Task Analysis - An analysis and listing of all the things people will do in a system, procedure, or operation with details on: (a) information requirements; (b) evaluations and decisions that must be made; (c) task times; (d) operator actions; and (e) environmental conditions.

Informal Review - A review of a program/project, task, or work unit not designated as formal by a cognizant convening authority per the formal review criteria.

Inheritance Review - A review to verify that inherited hardware, or an inherited hardware design, is adequate to satisfy the requirements of the inheriting program/project.

Inherited Hardware - Hardware built for a previous program/project to be used in an appropriate application by the inheritor.

In-house Program/Project - A program/project that is implemented within the customer organization rather than by a system or integration contractor.

Interface - The boundary, often conceptual, between two or more functions, systems, or items, or between a system and a facility, at which interface requirements are set.

Item - Any product including processes and facilities.

Life Cycle Cost - The total cost of acquisition, operation, maintenance, and support of an item throughout its useful life, and including the cost of disposal.

Link Analysis - A method for arranging the physical layout of instrument panels, control panels, workstations, or work areas to meet specific objectives; e.g., increased accessibility. An assessment of the connection between (a) a person and a machine or part of a machine, (b) two persons, or (c) two parts of a machine.

Logistics - The discipline dealing with the support related activities of the procurement, maintenance, and transportation of equipment, supplies, facilities, and personnel.

Logistics Support - The management and technical process by which all elements of logistics are planned, acquired, tested, and deployed in a timely and adequate manner.

Logistics Support Cost - The cost of providing all support considerations necessary to assure the effective and economical support of systems for their life cycle.

Maintainability - A measure of the ease and rapidity with which a system or equipment can be restored to operational status following a failure. It is characteristic of equipment design and installation, personnel availability in the required skill levels, adequacy of maintenance procedures and test equipment, and the physical environment under which maintenance is performed. One expression of maintainability is the probability that an item will be retained in or restored to a specified condition within a given period of time, when the maintenance is performed in accordance with prescribed procedures and resources.

Maintainability, Demonstrated - Maintainability which has been measured by the use of objective evidence gathered under specified conditions.

Maintainability, Predicted - Maintainability which is expected at some future time, postulated on analysis, past experience, and tests.

Maintainability Prediction - A forecast of the maintainability of a system or system element.

Maintenance - All actions necessary for retaining an item in, or restoring it to, a specified condition.

- **Maintenance, Corrective** – All unscheduled maintenance actions, performed as a result of system/product failure, to restore the system to a specified condition.
- **Maintenance, Organizational** – Maintenance performed by the using organization. Includes routine inspection, servicing, minor repairs and adjustments.
- **Maintenance, Preventive** - All maintenance actions performed to retain an item in a specified condition, including periodic inspection, detection, condition monitoring, calibration, and critical item replacement to prevent incipient failures.
- **Maintenance, Scheduled** - A form of preventive maintenance.
- **Maintenance, Unscheduled** - Corrective maintenance.

Maintenance Analysis - The process of identifying required maintenance functions by analysis of the design, and to determine the most effective means to accomplish those functions.

Maintenance Concept - A description of the planned general scheme for maintenance and support of an item in the operational environment. The maintenance concept provides the basis

for design, layout and packaging of the system and its test equipment and establishes the scope of maintenance responsibility for each level of maintenance category and the personnel resources required to maintain the system.

Maintenance Manpower Cost - The cost of the labor (as opposed to material) to retain an item in, or restore it to a specified condition.

Maximum Corrective Maintenance Time (MmaxCT) – The maximum time required to complete a specified percentage of all maintenance action. Also (from Mil Std-471), “That value (of maintenance downtime) below which a specified percent of all maintenance (actions) can be expected to be completed. Unless otherwise specified, this value is taken at the 95th percentile point of the distribution of downtimes.”

Maximum time to repair (maxTTR) - A measure of that time below which a specified percentage of all corrective maintenance tasks must be completed. When stated as a requirement, the max TTR should be stated for organizational and direct support levels of maintenance. Max TTR is used as an “on-system” maintainability parameter; it is not used for the off-system repair or replaced components.

Mean Downtime – The combination of all times involved in restoring an equipment to operation. Mean downtime includes Active Corrective Maintenance, Logistics Downtime, and Administrative Downtime.

Mean-Time-Between-Failures (MTBF) - A basic measure of reliability for repairable systems, MTBF is the mean number of life units during which all parts of the system perform within their specified limits, during a particular measurement interval, under stated conditions. - The mean of the distributions of the time interval between failures.

Mean-Time-To-Repair (MTTR) - A basic measure of the capability to actively repair a device or system, MTTR is a design quantity representing the onsite repair time only, without consideration for acquisition of spare parts and other logistics-related functions not considered part of active repair. MTTR is the mean of the distributions of the time-intervals needed to repair an item. This is often computed as the accumulation of active repair times divided by the total number of malfunctions during a time interval.

Metric - A measure used to indicate progress or achievement.

Milestone - Any significant event in the program/project life cycle or in the associated reliability or maintainability program which is used as a control point for measurement of progress and effectiveness or for planning or redirecting future effort.

Mission Critical - An item or function, the failure of which may result in the inability to retain operational capability for mission continuation if a corrective action is not successfully performed.

Mission Profile - A time phased description of the events and environments an item experiences from initiation to completion of a specified mission, to include the criteria of mission success or critical failures. Mission Profiles are used in establishing general performance requirements and are essential to evaluate R&M performance. They should include functional and environmental profiles that define the boundaries of the R&M performance envelope, provide the timelines typical of operations within the envelope, and identify all constraints where appropriate.

Operational Readiness - The ability of a system to respond and perform its mission upon demand.

Part - One piece, or two or more pieces joined together, which cannot be disassembled without destruction or loss of design use

Performance - A measure of how well a system or item functions in the expected environments.

Performance-Based Contracting - The method of contracting which entails structuring all aspects of an acquisition process around the purpose of work to be performed as opposed to how the work is to be performed. It emphasizes objective, measurable performance requirements and quality standards in developing statements of work, selecting contractors, determining contract incentives, and performance of contract administration..

Problem/Failure Management - A formalized process to document, resolve, verify, correct, review and archive problems and failures incurred during the development of functional hardware or software.

Procedure - A documented description of a sequence of actions to be taken to perform a given task.

Process Failure Modes and Effects Analysis (FMEA) - An analysis of an operation/process to identify the kinds of errors humans could make in carrying out the task. A method to deduce the consequences for process failure and the probabilities of those consequences occurring.

Product - A result of a physical, analytical, or other process which is intended for use. What is delivered to the customer (e.g., hardware, software, test reports, data), as well as the processes (e.g., system engineering, design, test, logistics) which make the product possible.

Program - An activity within an Enterprise having defined goals, objectives, requirements, funding, and consisting of one or more projects, reporting to the NASA Program Management Council (PMC), unless delegated to a Governing Program Management Council (GPMC).

Program Management Council (PMC) - The Senior Management group, chaired by the Deputy Administrator, responsible for reviewing, recommending approval of proposed programs, and overseeing their implementation according to Agency commitments, priorities, and policies.

Program/Project Management Process - The NASA process for the successful accomplishment of programs/projects through customer satisfaction with the products delivered.. It includes the following subprocesses:

Program/Project Formulation - Defines an affordable program/project concept and plan to meet mission objectives or technology goals specified in the program/project plan.

Program/Project Approval - Determines whether a program/project is ready to proceed from Formulation to Implementation.

Program/Project Implementation - Implements the approved program/project requirements and plans. Implementation culminates in the delivery of the program/project products and services to the customer.

Program/Project Evaluation - Provides an independent assessment of the continuing ability of the program/project to meet its technical and programmatic commitments and to provide value-added assistance to the program/project manager as required. Evaluation is applied throughout the life cycle of programs/projects and consists of the planning and conducting of reviews and assessments during the formulation and implementation of a program/project.

Program/Project Surveillance Plan (PSP) - Documentation of the overall approach used by the program/project for the maintenance of government insight of contractor performance on the program/project.

Project - An activity designated by a program and characterized as having defined goals, objectives, requirements, Life Cycle Costs, a beginning, and an end.

Purchaser - In a contractual relationship, the recipient of a product or service provided by a supplier.

Redundancy (of design) - A design feature which provides a system with more than one function for accomplishing a given task so that more than one function must fail before the system fails to perform the task. Design redundancy requires that a failure in one function does not impair the system's ability to transfer to a second function.

Reliability - The probability that an item will perform its intended function for a specified interval under stated conditions. The function of an item may be composed of a combination of individual sub-functions to which the top level reliability value can be apportioned.

Reliability Analyses - A set of conceptual tools and activities used in reliability engineering.

Reliability Assurance - The management and technical integration of the reliability activities essential in maintaining reliability performance, including design, production, and product assurance activities.

Reliability Centered Maintenance - An on-going process which determines the mix of reactive, preventive, and proactive maintenance practices to provide the required reliability at the minimum cost. It can use diagnostic tools and measurements to assess when a component is near failure and should be replaced. The basic thrust is to eliminate more costly unscheduled maintenance and minimize preventive maintenance.

Reliability, Demonstrated - Reliability which has been measured by the use of objective evidence gathered under specified conditions.

Reliability Prediction - A forecast of the reliability of a system or system element, postulated on analysis, , past experience, and tests.

Requirements - A set of characteristics or distinguishing features that is obligatory or a necessity. In engineering, requirements are established to meet operational needs and comply with applicable policy and practices.

Review - A critical examination of a task or program/project to determine compliance with requirements and objectives.

Risk - A combination of the likelihood of an undesirable event occurring and the severity of the consequences of the occurrence.

Risk Acceptance - The act by a decision maker of accepting a risk because the benefits outweigh the perceived risk.

Risk Assessment, Probabilistic - An evaluation of a risk item which determines (1) what can go wrong, (2) how likely is it to occur, and (3) what are the consequences. Assessment methods include:

- **Risk Assessment, Qualitative** - A process which assigns qualitative risk measures like "high, medium, and low" to both the probability and the adverse consequences of items on a Significant Risk List. These measures are often displayed in matrix format and could be relative to past programs/projects or could be probability ranges. These subjective assessments cannot be used for aggregating risks, and cannot be used for making quantitative tradeoffs.
- **Risk Assessment, Quantitative** - The process of assigning proportional numerical quantities to both the likelihood and the adverse consequences of risk items.

Risk Management - An organized means of controlling the risk on a program/project.

Risk Mitigation – The process of reducing either the likelihood or the severity of a risk because the benefits from assuming the risk do not outweigh the perceived risk.

Simulation - The process of conducting experiments with a model (an abstraction or simplification) of an item, within all or part of its operating environment, for the purpose of accessing its behavior under selected conditions or of evaluating various strategies for its operation within the limits imposed by developmental or operational criteria.

Single Failure Point - A single element of hardware, the failure of which would result in loss of mission objectives, system function, hardware, or crew as defined for the specific application or program/project.

Single Failure Point Policy - Program/project policy requiring that no success-critical failure points be permitted in a system design

Single Process Initiative - A program for the elimination of agency-unique processes or systems, imposed on contractor facilities shared by multiple Federal government agencies. All contractor systems and processes are candidates for this initiative where improved efficiency will result.

Software Reliability - See the definition for reliability. Since it is very difficult to verify that software operates under conditions which match the "stated conditions," software reliability performance requirements are not often specified. More common are software quality assurance requirements such as defects per 1000 lines of code.

Spares - Maintenance replacements for parts, components, or assemblies in deployed items of equipment.

Specification - A description of the essential technical requirements for items (hardware and software), materials, and processes that includes verification criteria for determining whether the requirements are met.

Statement of Work (SOW) - The part of a contract which lists the specific tasks to be performed by the contractor.

Stress Screening - The process of applying mechanical, electrical, or thermal stresses to an equipment item for the purpose of precipitating latent part and workmanship defects to early failure.

Subsystem - A grouping of items satisfying a logical group of functions within a system.

Supplier - Any organization which provides a product or service to a *customer*. By this definition, suppliers may include vendors, subcontractors, contractors, flight programs/projects, and the NASA organization supplying science data to a principal investigator. (In contrast, the classical definition of a supplier is: a subcontractor, at any tier, performing contract services or producing the contract articles for a contractor.)

Support Equipment - Equipment required to maintain systems in effective operating condition in its intended environment, including all equipment required to maintain and operate the system and related software.

Surveillance: The continual monitoring and verification of status of an entity and analysis of records to ensure specified requirements are being met. Surveillance activities may be delegated to other parties on behalf of the customer. It may be 100% , statistically-based sampling, qualitative sampling or the result of discussion with individuals who have first hand knowledge. It also may include the monitoring of contractor supplied metrics, available contractor data, sampling, or surveys.

System - An integrated aggregation of end items, interfaces, and support functions designed to fulfill a specific mission requirement. A system may include equipment, trained personnel, facilities, data and procedures, and software. For program/project purposes, a system is typically defined as the highest level of hardware organization composed of multiple subsystems. The term is also used to describe a disciplined and consistent approach to accomplish a task, e.g., a failure reporting system.

Tailoring - To make, alter, or amend for a particular end or purpose. In performance-based contracting, the process by which sections, paragraphs, and sentences of specifications, standards, and other requirements and tasking documents are evaluated to determine the extent to which they are applicable to a specific acquisition contract and then modified to balance performance, cost, schedule, and risk.

Task - A function to be performed. In contract proposals, a unit of work that is sufficiently well defined so that, within the context of related tasks, readiness criteria, completion criteria, cost and schedule can all be determined.

Test - A procedure for critical evaluation; a means of determining the presence, quality, or truth of something; a trial. In engineering, a method of determining performance by exercising or operating a system or item using instrumentation or special test equipment that is not an integral part of the item being tested.

Testability - A design characteristic which permits timely and cost-effective determination of the status (operable, inoperable or degraded) of a system or subsystem with a high level of confidence. Testability attempts to quantify those attributes of system design which facilitate detection and isolation of faults that affect system performance.

Tradeoff Analysis - An objective comparison, with respect to performance, cost, schedule, risk, and all other reasonable criteria, of all realistic alternative requirements; architectures; baselines; or design, verification, manufacturing, deployment, training, operations, and support approaches.

Troubleshooting - A procedure for localizing and diagnosing equipment malfunctions or anomalies, typically by a systematic examination progressing from higher to lower levels of assembly.

Unit - An assembly of any combination of parts, subassemblies, and assemblies mounted together, normally capable of independent operation in a variety of situations.

Uptime - The total time a system is in an operable and committed state.

Validation- To establish the soundness of, or to corroborate. Validation testing of products is performed to ensure that each reflects an accurate interpretation and execution of requirements and meets a level of functionality and performance that is acceptable to the user or customer.

Verification - The task of determining whether a system or item meets the requirements established for it.

3.2 ACRONYMS

BIT	Built-in-Test
CCB	Configuration Control Board
CDR	Critical Design Review
CDRL	Contract Deliverables Requirements List
DCMC	Defense Contract Management Command
FDIR	Fault Detection, Isolation and Recovery
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects, and Criticality Analysis
FRACAS	Failure Reporting and Corrective Action System
FRR	Flight Readiness Review
FTA	Fault Tree Analysis
GPMC	Governing Program Management Council
HEDS	Human Exploration and Development of Space Enterprise
LCC	Life Cycle Cost
LRU	Line Replaceable Unit
MCR	Mission Concept Review
MDT	Mean Downtime
MmaxCT	Maximum Corrective Maintenance Time
MTBF	Mean Time Between Failure
MTTR	Mean Time to Repair, Mean Time To Restore
NASA	National Aeronautics and Space Administration
NPD	NASA Policy Directive
NPG	NASA Procedures and Guidelines
PDR	Preliminary Design Review
PMC	Program Management Council
PSP	Program/Project Surveillance Plan

R&M	Reliability and Maintainability
RMP	Risk Management Plan
SOW	Statement of Work
STD	Standard
T&E	Test and Evaluation

CHAPTER 4 - GENERAL

4.1 NASA R&M Policy

NASA Policy Directive (NPD) 8720.1, "NASA Reliability and Maintainability (R&M) Program Policy," describes the R&M policies that apply to all NASA Enterprises, Centers, and Institutional Programs. This policy is based on the understanding that NASA has a business objective to obtain products and services at a high level of excellence at minimum cost. A R&M investment provides benefits throughout mission life which may not be immediately evident during development and production. For example, correcting a design flaw after deployment costs many times the cost of correcting it during design. It is management's responsibility to translate system performance requirements into an effective R&M program.

4.2 R&M Approach

The current NASA approach to R&M described throughout this standard is based on the requirements of NASA Procedures and Guidelines (NPG) document 7120.5A and several initiatives related to the acquisition process, such as performance-based contracting, the single process initiative, an increased interest in risk management, and imposition of realistic metrics to better define accomplishment of objectives. The processes defined in NPG 7120.5A are no longer based on rigidly defined program/project phases and milestones. Each program/project must now define an acquisition approach tailored to its specific needs. Performance-based contracting places responsibility on the supplier for mission success by emphasizing contracting for results instead of contracting for "best effort." Formerly, the customer specified the major R&M engineering, analysis, and test related tasks comprising an R&M program, and suppliers were evaluated on their performance of these tasks. Now, customers will include objective R&M performance requirements as a part of the mission performance requirements contained in the specifications and statement of work. These mission performance requirements are the minimum performance level acceptable to the government. Satisfying the contract is defined as meeting these requirements (or demonstrating the equipment's ability to meet these requirements). The mere performance of R&M tasks does not by itself constitute contract compliance. Even with these changes in NASA policies and approach, the application of an R&M program will generally follow the generic process illustrated in Figure 4-1 and described in the following:

1. *Identify desired outcomes.* By emphasizing objective and measurable outcomes based on the program/project mission requirements, an acquisition centers on the purpose of the contracted work and, more importantly, the results of that work.
2. *Select measures and indicators.* Establishing measures and indicators sets the stage for later evaluations. Although the desired performance and surveillance standards may change as program/project perturbations occur, the associated measures and indicators will likely remain the same, providing a level of continuity for the program/project.
3. *Set performance and surveillance standards.* R&M performance requirements are defined in terms of a system's quantitative R&M performance, programmatic/mission requirements, and operating environments, all with an emphasis on the selected measures and indicators. Equally important to including proper R&M requirements in the

Statements of Work (SOW) is ensuring that surveillance plans are established and implemented early in the program/project.

4. *Report results.* Results of the surveillance effort are reported to support assessment of the progress made toward meeting requirements.
5. *Use results for planning, managing and budgeting.* Assessing progress toward meeting requirements provides the feedback needed to adjust planning, managing and budgeting of the program/project.

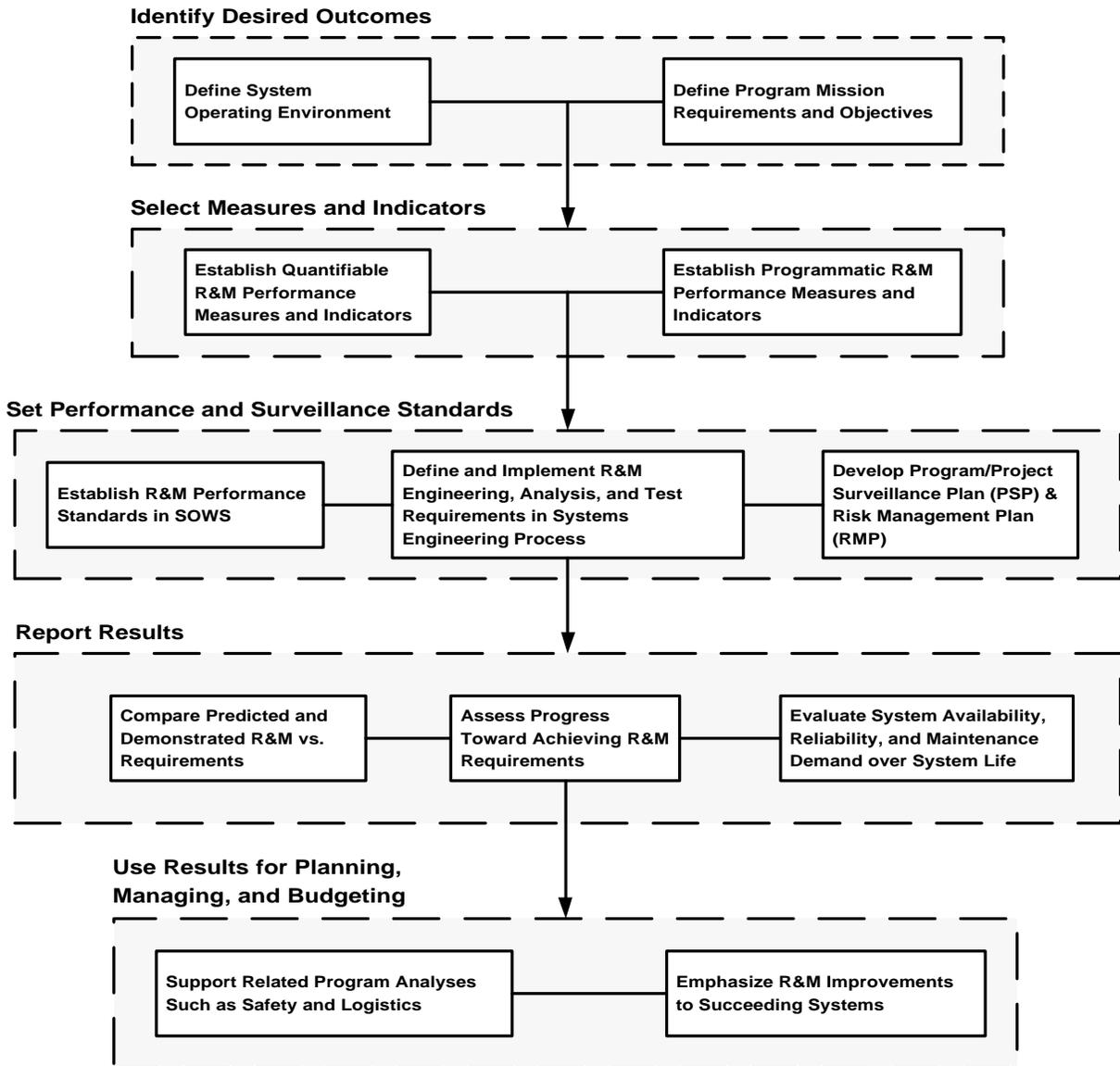


Figure 4-1 Generic R&M Process

Appendix A provides a series of matrix-based R&M “Toolsets” that provide brief descriptions of analyses and activities that have proven effective on past programs. Each “tool” is accompanied by brief synopses of what the tool does, why it is used, when it is called for, and when during a program/project it is performed. In compliance with performance-based-contracting methodologies, these analysis techniques and activities are not to be specified in lieu of R&M performance requirements. Appendix A should not be construed as a requirement, it is provided for information only. While contractors are at liberty to use any of the methods, they also are encouraged to develop and use their own R&M techniques.

One additional aspect to be considered is the impact of the revised acquisition process and performance-based contracting on risk management. As described in subsequent chapters, R&M is a major contributor to the overall risk management program. In the past, NASA has managed risks by closely specifying and monitoring how contractors work. This approach may have seemed prudent to minimize risks, but minimal risks can lead to minimal returns. Although NASA still retains the ultimate responsibility to procure the best value for the taxpayer dollar, the new process of holding contractors accountable for their final product transfers much of the cost, risk, and quality responsibility from NASA to the contractor. While NASA is responsible for defining its need through the SOW or specifications, the contractor is encouraged to improve its processes and to realize greater profits through incentives. Risk management plans and analyses may need adjustments to address the shift in risk and responsibility. The key is to establish an effective government surveillance program that provides adequate confidence in the contractor's performance, but minimizes NASA's intrusion into the contractor's day-to-day processes. However, NASA can still use selective oversight of specific programs/projects to assure that high risk, high cost programs/projects meet their required performance requirements.

4.3 R&M Customer

NASA's R&M emphasis has shifted from imposition of inflexible requirements to a focus on customer needs. Consumers of R&M products and services range from internal customers, who use outputs such as analyses and studies, to external customers to whom end items meeting R&M performance requirements are delivered. For example, the R&M customers for a spaceflight mission may include the flight program/project, the mission sponsor, and the consumers of science data and mission results, including the principal investigator and the public. R&M decision makers include the program/project manager, R&M engineers, and procurement staff in both the customer and supplier organizations.

The design of an effective R&M program will require communication with the customer to identify true customer expectations for system performance and consideration of cost-effective strategies for attaining performance-based objectives. Historically, this process was relatively easy as applied to development of NASA flight and ground systems because R&M program requirements were largely predetermined based on the criticality classification of the mission. Instead of criticality, total mission cost or life cycle cost has become a more significant factor in the sponsorship of non-HEDS programs/projects. As a result, R&M program resources have become more constrained. The customer expects a supplier to manage risk by selecting and implementing only those R&M program elements which offer a high return. Those suppliers which are most effective in managing risk and satisfying customer expectations will be assigned future responsibilities and recognized for their contribution to the NASA community.

4.4 R&M Training

This standard provides some of the basic information necessary to develop and implement an R&M program; however, effective implementation depends upon the capabilities of the individuals assigned to the program/project. Program/project and institutional organizations are encouraged to support general and advanced training of their staff in the R&M disciplines for the purpose of:

- Acquainting design engineers and engineering managers with the benefits of applying R&M principals and practices.
- Advancing professionalism within the R&M program organization by establishing standards for acceptable R&M engineering practices.
- Providing advanced training in the R&M disciplines to augment principal engineering disciplines training (e.g., mechanical, electrical, industrial engineering). This may include advanced study of FMEAs, fault trees, the mathematical background to R&M concepts, and the integration of R&M activities into the NASA system engineering approach to product development.
- Disseminating information on the latest R&M tools, such as commercial application software for concurrent engineering.
- Familiarizing the engineering staff with new and innovative approaches to R&M assurance consistent with the changing NASA program/project development environment.
- Providing a thorough understanding of the impact of internal and external environments on product reliability

Information concerning training in the R&M discipline and other Safety and Mission Assurance (SMA) disciplines can be obtained at the Safety and Mission Assurance portion of the NASA Site for On-line Learning and Resources web site (<http://www.solar.msfc.nasa.gov>)

CHAPTER 5 - R&M OVERVIEW

5.1 R&M and the Acquisition Process

With the advent of NPG 7120.5A, the acquisition process was changed from the original rigid, five-sequential-phase process (A - Preliminary Analysis, B - Definition, C - Design, D - Development, and E - Operations) to four highly interactive subprocesses (Formulation, Approval, Implementation, Evaluation). Emphasis is on tailoring of concurrent activities to meet the specific needs of a program/project. R&M considerations represent one subset of objectives and accomplishments that are integrated with engineering, operations, scheduling, procurement, and risk factors to ensure affordability, fulfillment of strategic goals and plans, and compliance with cost/schedule/technical commitments

Program/project concepts, requirements, and plans are produced during Formulation and are independently evaluated to support approval of the program/project to proceed to Implementation. Knowledge generated through scientific or technical research, combined with strategic planning, policy development, and allocation of resources, provides the input for the trade-offs needed to yield optimum performance requirements. Independent evaluations support initial Approval and continue to support the process through Implementation as design of the program/project elements is finalized and hardware is produced, integrated, and placed into operation.

Figure 5-1 places the R&M program in a customer/supplier orientation within the framework of the four acquisition subprocesses. It must be emphasized that within this framework each program/project must tailor R&M to its own needs. The remainder of this chapter focuses on an overview of R&M considerations in the overall acquisition process. Subsequent chapters expand upon the appropriate parts of the flow diagram to illustrate the activities involved, and provide guidance for tailoring the R&M program.

5.1.1 Formulation

The objective of Formulation is to define an affordable program/project concept and plan to meet mission objectives or technology goals. From an R&M perspective this process includes many activities that will define the level of complexity of the R&M program. For example, during Formulation, the initial program/project metrics will be identified and the structure of the program/project reviews will be established. Additionally many of the activities performed during Formulation , such as trade studies, initial life-cycle costing and identification of preliminary risks and risk mitigations may require support from the R&M disciplines. Formulation supports derivation of the R&M plan for program/project implementation and the R&M measures, indicators, quantifiable performance criteria, and programmatic stipulations. During this entire process the customer prepares and refines its Risk Management Plan (RMP) as defined NPG 7120.5A and, if appropriate, a Program/Project Surveillance Plan (PSP). The Government maintains insight into the contractor's work through the multi-functional RMP and PSP. These rely increasingly on evaluating contractor generated internal data. The RMP provides the process and operational details of how the risk management effort will be accomplished along with processes, methods, tools, and metrics to be used in identification, control and mitigation of risk. The PSP includes the basis and groundrules for evaluating and assessing contractor progress

toward completion of the plan of actions, and contractor progress toward achieving the required R&M performance.

During Formulation the contractor responds to the customer's RFP with an analysis of early design requirements, the overall R&M Program plan and R&M Program Performance Evaluation Plan, and a description of how risk will be managed (the RMP). Top level R&M performance

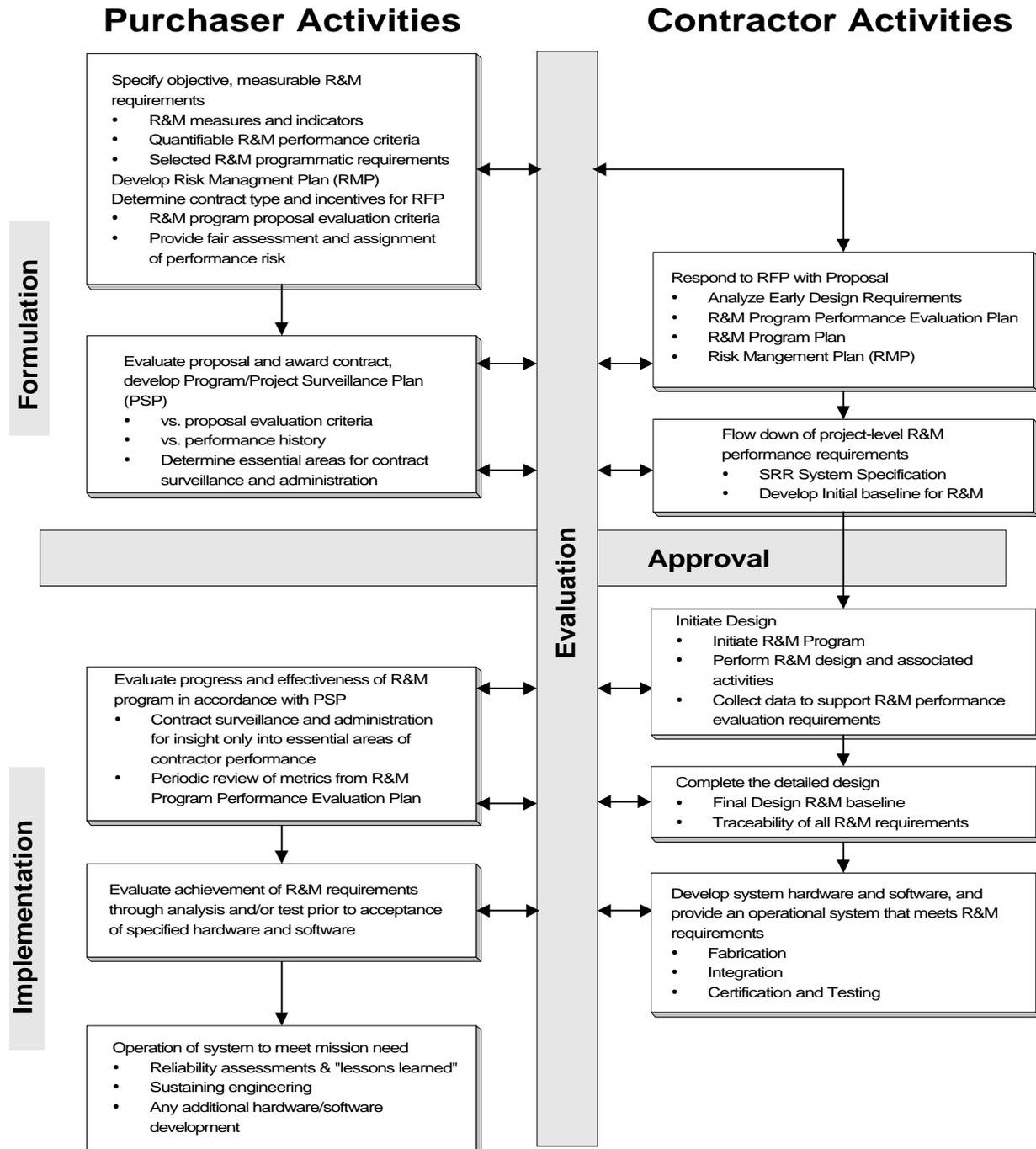


Figure 5-1. R&M Program within the Acquisition Subprocesses

requirements are also apportioned to the primary hardware/software blocks, included in the System Requirement Review Specification. and used to develop the initial R&M baseline for use in the Approval process.

5.1.2 Approval

The objective of Approval is to initially decide on program/project readiness to proceed from Formulation to Implementation. Information from the Formulation and Evaluation subprocesses, including R&M information gathered during reviews or program/project planning, will be used to support program/project approval to transition from Formulation to Implementation. Since Approval takes place at a high level, direct R&M involvement will be minimal other than to have provided supporting information and activities to the decision makers during Formulation and Evaluation.

5.1.3 Implementation

The objective of Implementation is to deliver the program/project products and capabilities specified in the approved program/project requirements and plans. This can be divided into three major categories of functions:

- **Completion of the detailed system design.** It can include products such as simulated and physical mock-ups and test articles of critical systems and subsystems; complete detailed system and component specifications, systems baseline description, and comprehensive requirements traceability of all derived requirements to parent (customer) requirements. Implementation of the RMP and PSP will also be used to assure that the contractor achieves the required R&M performance.
- **Development of the system hardware and software and delivery of an operational system that is acceptable to the ultimate user.** This comprises the fabrication, integration, certification and testing of all system hardware/software required to provide for system initiation and subsequent operations. The RMP and the PSP continue to be major influences in monitoring contractor activities during early Implementation and are coupled with analyses and tests to measure and evaluate achievement of the required R&M performance prior to acceptance of specified hardware and software.
- **Satisfaction of mission need throughout operations and, ultimately, disposal of the systems.** R&M activities continue during Implementation for logistics support, sustaining engineering, and to document “lessons learned.”

5.1.4 Evaluation

The objective of Evaluation is to provide timely assessment of the continuing ability of the program/project to meet its technical and programmatic commitments. It also provides value-added assistance to the program/project manager as required. A major portion of this process is the continuing assessment of work initiated during Formulation. Specifically this includes the use of program/project metrics, life-cycle cost models and risk management analyses, all of which can include elements of R&M. Evaluation continues concurrently with Implementation, in the form of reviews that measure program/project performance against program/project plans. Although each

program/project defines its own review structure, these reviews are expected to include “typical” reviews such as the Preliminary Design Review (PDR) and Critical Design Review (CDR). These reviews would address progress toward meeting R&M performance requirements and other requirements that are related to R&M (e.g., safety, logistics, and maintenance requirements).

5.2 R&M Integration With Other Organizational Elements

Integration of R&M with other organizational elements throughout a system’s life cycle is an essential management process used to ensure that requirements are met expeditiously and economically. Integration includes coordinating efforts, establishing/controlling/verifying interfaces between mating equipments, eliminating redundant activities, and facilitating the flow of information. Integration activities with all program/project elements ensure that R&M engineering techniques and practices are applied appropriately during hardware and software system development and integration/verification to assure the achievement of all R&M performance requirements. As a program/project develops during Formulation, the program/project manager will develop the structure for the program/project and establish the foundation for integration of the associated disciplines.

R&M engineers need to understand how the R&M discipline interfaces with other disciplines in order to assist the program/project manager with the development of the R&M Program. Integration of R&M is a key feature of the program/project and should be considered in the development and implementation of the RMP and PSP. Through an integrated approach, R&M Engineering is able to influence other activities, such as manufacturing, human engineering, safety, diagnostics and maintenance, logistic support, and software development. Working arrangements between R&M Engineering and other activities should be established to identify mutual interests, maximize benefits of mutually supporting tasks, and minimize effort overlap. Such organizational working relationships can also promote more system-oriented decisions when the work is properly integrated at higher levels.

The following paragraphs highlight the relationship between R&M and the organizational elements of a program/project.

5.2.1 Manufacturing and Quality Assurance

A primary R&M concern during manufacturing is to prevent degradation of the inherent reliability and maintainability designed into the product during Formulation and Implementation. The Quality and Product Assurance activities should work closely with the R&M development team to assure a full understanding of the impact of the manufacturing processes on end item R&M and to develop value added manufacturing processes that assure the integrity of the product. These provisions should not only continuously improve product quality, but should also ensure capable and controlled program/project critical manufacturing and operational processes. Involvement of R&M Engineering in the review/approval loop for the selection of parts and materials, manufacturing processes and procedures, and assembly procedures further ensures that R&M concerns are addressed.

5.2.2 Human Engineering

Human factors engineering is concerned with the interactions between the human element and the hardware/software of the system. Human factors engineering involves selecting and/or designing maintenance and operational features that consider anthropometric factors, human sensory factors, human physiological factors, and human psychological factors. R&M performance requirements will drive much of the human engineering effort, and design decisions related to the features of these human factor features will have an especially strong influence on design for maintainability. Effective coordination between Human Factors Engineering and R&M Engineering is essential to ensure maximum performance from personnel so that the desired levels of R&M may be realized throughout the life of the system.

5.2.3 Safety

R&M engineers and safety engineers have a common interest in the identification of hardware and software failure modes and hazards, along with their potential effect(s). An interface between these two disciplines and design engineering will ensure the timely communication of all potential hazards, and provide for the early identification and correction of problems inherent in the proposed design. Safety engineers use R&M data in development of hazard analyses that identify and address all hazards resulting from the failure modes. R&M engineering should review the hazard analyses to ensure that reliability and/or maintainability are not degraded by the resulting design recommendations.

5.2.4 Diagnostics And Maintenance

The various R&M analyses, such as FMEA, reliability predictions, and maintainability predictions are a significant source of information in designing a diagnostics system and maintenance plan. An important component of maintainability is testability, defined as a design characteristic that allows the status (operable, inoperable, or degraded) of an item to be determined and the isolation of faults within the item to be performed in a timely and efficient manner. A system's testability, coupled with its degree of built-in-test, both influences and is influenced by R&M performance requirements. Increased complexity and higher demands of NASA systems have highlighted the importance that diagnostics has in developing faster, better, cheaper systems. Decisions arising from the development of diagnostic systems, and the corresponding maintenance procedures may require updating of the R&M analyses and should be fed back to R&M engineering on a timely basis.

5.2.5 Logistic Support

Logistic Support is concerned with all aspects of an acquisition that relate to designing a system to be supported once it becomes operational. This includes not only the development of an equipment itself, but its supporting facilities and equipment, the maintenance and operation infrastructure, and provisions for final disposition of the entire system at the end of its life cycle. The goal of logistic support is to ensure that a system is able to be used to the greatest extent possible. Logistic support analyses and decisions (such as sparing) are dependent on reliability and maintainability prediction data. It is important to the success of the logistics program that a close working relationship be established early in the program/project among R&M, Logistics, and Engineering groups to ensure a timely exchange of information.

5.2.6 Software

The life-cycle of computer software covers the period from its conception until the time it is no longer available for use. Software is seldom static, and long after a system has become operational and is in use, upgrades to its software are likely to be made to increase performance or take advantage of new technology. Software R&M is concerned with the initial release and subsequent upgrades of software to ensure that minimal downtime is attributed to the software. R&M performance requirements should be specified for software as well as hardware. The resulting tradeoffs among hardware, software and operations become an important aspect of R&M and System Engineering. Close coordination of all design, development, operational and support decisions among Hardware, Software, and R&M groups is essential for achievement of software R&M performance requirements.

5.2.7 Program/Project Engineering

R&M engineers and project engineers have a common interest in the identification of risks and hardware and software failure modes, along with potential effect(s). An interface between these two disciplines will ensure timely communication of all potential risks, provide early identification, and aid in development/application of methods to mitigate the risk inherent in the proposed design. Project engineers use R&M data for risk identification and analysis that identifies and addresses all risks resulting from the possible failure modes. R&M engineering should review the risk mitigation methods to ensure that reliability and/or maintainability are not degraded by the resulting risk mitigation method.

5.3 Acquisition Initiatives Related to R&M

Many of the initiatives being implemented in the Acquisition subprocesses have an impact on R&M. These initiatives may be a major factor in the structure and implementation of the overall program/project, and consequently the R&M program. The following paragraphs describe some of the major initiatives and the impact that they have on R&M.

5.3.1 Performance-Based Contracting

Performance-based contracting is an approach to acquiring products and services which resembles that used by commercial industry.² Performance-based requirements involve quantitative measures of product performance such as the number of failures over time, life expectancy, and time to repair a product within specified environmental constraints. With this approach, the customer does not stipulate how a supplier is to meet the requirements. This encourages contractor innovation, use of best available design and manufacturing practices and technology within cost limitations, and elimination of activities which do not add value to the product. This approach does not absolve the customer from responsibility for insight into contractor processes, including review of a supplier plan for achieving the reliability and maintainability performance requirements, as well as periodic review of progress toward meeting the performance requirements.

² "Performance-Based Contracting," letter from Daniel S. Goldin, NASA Administrator, March 18, 1996. (<http://www.hq.nasa.gov/office/codeq/aqshp/goldinwp.pdf>)

Transition from the existing customer/supplier relationship to a performance-requirement driven partnership places increased responsibility on the supplier to develop and implement a R&M program effective in achieving specific availability and lifespan requirements. The customer role in this partnership emphasizes specifying the system R&M performance requirements and assessing the supporting processes and resultant design to assure that these performance requirements are met. The supplier is responsible for defining, documenting, and implementing an approach that will ensure that mission assurance activities are accomplished and are effective in the mitigation of mission risk.

5.3.2 Risk Management

Given the broad consequences of mission risk -- reduced spacecraft performance, cost increases and schedule delays, and injury to life and property -- an effective R&M program must include defined activities for assisting in maintaining risks within managed boundaries. The risk management process should provide a methodology for balancing program/project risks by the selective application of tradable programmatic resources (e.g., safety, reliability, maintainability, quality, and performance) and design characteristics so as to achieve mission success. The major risk management activities -- risk planning, identification and assessment, decision making, and tracking -- should be reiterated throughout the program/project life cycle as new risks are identified and old risks are retired, changed in magnitude, or realized. NASA seeks to strengthen this risk management process to accommodate use of relatively unproven technology in the design of low cost, short duration missions.

The approach to risk management should integrate safety, reliability, maintainability, and quality data and issues and correlate those data and issues with probability of mission success such that the supplier routinely considers risk in day-to-day decision making. Customers may hold suppliers accountable for risk management by means of auditable plans, system procedures, work instructions, and acceptable products and services which meet customer policies and requirements.

5.3.3 Metrics

Metrics assist in the evaluation of R&M performance and are essential to the identification and quantitative assessment of risk. It is the responsibility of the supplier to develop and maintain performance metrics which effectively indicate the level of success in execution of the contract requirements. The supplier proposes a scheme for metrics definition, correlation of the metrics to the quantitative requirements, and measurement of management responsiveness to the performance indicated by the metrics. An example of a performance metric is the achieved vs. desired amount of margin in a test program.

Performance metrics are augmented by “insight” metrics—those which are not contractually required but provide the customer R&M engineer with an indication of supplier performance through visibility into internal supplier processes and procedures. Such insight metrics available to the customer may be generated by characterization of the supplier’s production environment, including selection of design and manufacturing tools, problems defined, process characteristics, and product characteristics. An example of an insight metric is the verifiable progress of a software supplier toward the objectives of their Process Improvement Plan (e.g., meeting the requirements for Level 4 software process maturity).

5.3.4 Single Process Initiative.

The Single Process/Block Change initiative has been endorsed by both the Department of Defense and NASA as a cost-savings acquisition reform measure.³ The thrust of the initiative is to enable contractors to propose single processes that would meet the needs of multiple Government customers at a given plant. This would eliminate duplicative contractor systems and processes imposed by each customer's requirements. The initiative is expected to reduce contractor costs, improve process efficiencies, reduce product costs, and improve product quality. Additionally, the Single Process Initiative will increase both the efficiency and effectiveness of the Government surveillance effort, particularly in the areas of cost/schedule/earned value reporting, and quality audits and reporting. At contractor request, the Defense Contract Management Command (DCMC) is authorized to issue a contract modification implementing a block change to all affected contracts. NASA will cooperate with DCMC for the development and acceptance of single processes wherever possible.

5.4 Summation

The remaining four chapters of this standard develop specific details concerning NASA's recommended R&M approach. In particular, customer and supplier roles are defined with respect to the development of R&M requirements, design for R&M, and the R&M assessment process within the four acquisition subprocesses. They expand upon the life cycle activities of Figure 5-1 as they relate to R&M, and how to address R&M needs throughout the acquisition process. Emphasis is placed on cultivating an environment of contractor initiative to meet government needs by providing contractors more liberty to conduct their business, at the same time holding them responsible for results. Appendices A through D provide a list of typical analyses and activities for given R&M disciplines, R&M content for statements of work, and definitions / synopses of key R&M disciplines.

³ "Acquisition Reform: Single Process/Block Changes," letter from Daniel S. Goldin, NASA Administrator, May 17, 1996. (<http://www.hq.nasa.gov/office/codeq/aqshp/singproc.pdf>)

CHAPTER 6 - R&M IN FORMULATION

6.1 Goal of Formulation

The goal of Formulation is to define an affordable program/project concept and plan to meet mission objectives or technology goals specified in the Agency or enterprise strategic plans. In meeting this goal, Formulation identifies and examines the many ways that the mission objectives or technology goals can be met. R&M have a significant role in supporting the Program/project Manager as the program/project is defined and as the initial risk management activities are implemented.

6.2 Program Management Activities Related to R&M

NPG 7120.5A outlines the major activities that the Program/project Manager must accomplish during Formulation, including developing the acquisition strategy, developing the acquisition team, exploring implementation options, developing metrics and performance assessment criteria, performing initial life cycle costing, and developing the operations concept including initial logistics analyses. Each of these activities can benefit from the timely and effective application of R&M principles and analyses.

6.2.1 Developing the Acquisition Strategy

One of the initial activities that the program/project manager must perform is to develop the Acquisition Strategy for executing the program/project with particular emphasis on completion of Formulation. The Acquisition Strategy will lay out in basic terms the approach that the program/project will take to progress through Formulation and set the basis for the transition into Implementation. It is during this activity (and several of the activities described in the subsequent paragraphs) that the program/project manager will make the initial decisions on how to apply and tailor Agency policy requirements to the specific program/project. R&M personnel should assist in the interpretation and application of NASA R&M policies and practices, such as NPD 8720.1, to the overall program/project requirements. In addition to tailoring program/project requirements based on the criticality and risk associated with the acquisition, NASA programs/projects will benefit from innovative R&M Assurance processes that maximize cost efficiency. These processes should engage the program/project development teams to jointly develop value-added R&M provisions that are responsive to the needs of each program/project, while continuously improving quality of the product. The tailored program/project R&M discipline activities will be the basis for program/project requirements that may manifest themselves in many areas such as the program/project metrics, safety requirements, performance assessment criteria, and risk management planning and implementation. These requirements, or a selected set of the requirements, may be documented in the Program/Project Plan and in supporting documents such as specification, implementation plan, and design requirements. On large projects there may also be a separate Mission Assurance Plan that augments the Program/Project Plan or Risk Management Plan.

6.2.2 Developing the Acquisition Team

During Formulation, the program/project manager will identify the personnel that are necessary to take the program/project from Formulation to Implementation. In addition, Evaluation will be

initiated and appropriate independent assessment team(s) will also be formed. The team development needs to consider the program/project being developed, its schedule and how to best apply the elements of the R&M discipline to the inline and independent assessment/evaluation of the program/project. Each of the R&M discipline elements, Reliability Engineering, Environmental Requirements Engineering, Problem/Failure Reporting, Electronic Parts Engineering, Materials and Processes, and Maintainability Engineering will be applied to varying degrees based on the nature of the program/project. Appendix B defines these discipline elements. Note these are not rigid categorizations and variations may exist within various NASA Centers. These assignments should also consider the overall risk management strategy for the program and be integrated with the risk management program. Assignment of R&M personnel to these teams will also need to be coordinated with the appropriate Safety and Mission Assurance Enterprise Agreements (reference <http://www.hq.nasa.gov/office/codeq/qdoc.pdf>) and the related Center Annual Operating Agreements which define the levels of support that the Center Safety and Mission Assurance offices will provide to the Center and its programs/projects.

6.2.3 Exploring Implementation Options

Formulation is the time when programs/projects explore the conceptualization of the solutions to meet the program/project needs. This includes evaluation of alternate designs and the associated evaluation of the technological capabilities to meet those needs. R&M personnel should be expected to assist in the evaluation of the maturity of technology and the risk associated with using a specific technology within a program/project. R&M estimates or assessments can be used to provide a valid picture of the equipment and/or system end item operation and its design alternatives. Trade studies are performed among reliability, maintainability, safety, performance, system configuration, environmental use, and other system/equipment requirements to optimize the system design. These trade studies can also be used to refine the top level mission success criteria or performance criteria for the program/project. Depending on the size and scope of the program/project these success criteria may be further defined in R&M terms.

Toward the end of Formulation, equipment functional characteristics and operational requirements become better defined as system concepts, designs, and new technologies are investigated more thoroughly. This is the period where early development modeling, demonstrations, and operational assessments are conducted to reduce new program/project risks prior to entering Implementation. Selected system or product candidate design solutions are subjected to extensive study and analyses at this time. This is also the period where the system R&M trade studies and cost-benefits analyses are performed and evaluated. During this period, the system requirements for R&M performance must be refined to ensure that they are practical, realistic, measurable and affordable. The planning for tracking R&M as the program/project progresses through Implementation starts to take place toward the end of Formulation to provide a continuous picture of the entire R&M program.

6.2.4 Developing Program/Project Metrics and Performance Assessment Criteria

A set of R&M, or R&M-related, performance requirements should result during the examination of design options and the related trade studies. These will contain the baseline criteria that will be used to assess program/project performance and will establish the data or measurement information (metrics) necessary to implement the assessments. These R&M performance

requirements become the basis for quantitative and qualitative criteria for engineering design, system feasibility studies, failure mode identification, cost studies, trade-off decisions, and flight demonstration testing during Implementation. As a part of the program/project metrics approach an effective R&M data system should be incorporated early to permit assessment of the system R&M performance and to insure that all R&M data recorded during operations are appropriately disseminated, analyzed and evaluated.

Achieving high levels of equipment reliability is one of the most important objectives in new programs/projects as there is an ever-increasing interest in the final system design cost and the associated logistic burden. For this reason, R&M performance requirements cannot be constrained to the critical failures associated with mission performance. They must also address the total spectrum of reliability and maintainability from the standpoint of (a) failures affecting the ability of the system to perform its mission, (b) costs resulting from repair or replacement of failed items, and (c) whether the R&M performance requirements can actually be quantified, measured and verified at a reasonable cost.

There are various methods of specifying and documenting quantitative R&M performance requirements. The selection of R&M parameters must be tailored for each system under development. R&M performance requirements are basically composed of three separate and essential elements:

- system operational mode based on specific mission profiles that the system is required to complete;
- system failure definition consistent with the operational mode,
- the numerical values of the R&M parameters themselves.

R&M parameters used as top level performance criteria will generally use units of measurement related to: (1) operational readiness; (2) mission success; (3) maintenance manpower cost; and (4) logistics support cost. Typical parameters that are used to quantify R&M performance at this level of detail are listed in Table 6-1.

Very important to both operations in an existing program/project and to the initiation and development of a subsequent program/project is the acquisition and understanding of operational/test data (including root analysis of failures). Rigorous acquisition, grouping, and trending of data permits the purchaser (and the contractor) to understand the meaning of both failure and successes, to understand where in its life cycle the device is, and to select when preventive (as well as corrective) action should be taken. Proper development of data acquisition requirements and the subsequent acquisition and analysis provides expert knowledge for both independent and inline oversight and insight of a program/project. Robust performance data is the lifeblood of a strong, successful and cost effective program/project.

6.2.5 Performing Life Cycle Costing

The Life Cycle Costing (LCC) process is established and the initial LCC estimates are performed during Formulation. Reliability and maintainability analyses provide essential data required to perform LCC. Failure rates and restoration times are essential in projecting the logistics costs associated with a program/project. They impact redundancy decisions, the number of spares

required, the labor-hours required to restore items to operation, etc. R&M estimations and data are essential for a successful LCC effort. Early R&M involvement with the identification of the program metrics to be applied as well as the LCC effort will enhance the capability to effectively consider LCC in decisions concerning implementation or technology application.

6.2.6 Developing the Operations Concept

The initial operations concept will also be developed during Formulation. One element to be considered in the initial operations concept should be the maintenance concept to be used for the system. This is consistent with NPD 8720.1 which requires the development and documentation of the maintenance concept. The defined maintenance concept will influence the structure and

Table 6-1. Typical Reliability, Maintainability, and Availability Parameters Used to Quantify R&M Performance

<ul style="list-style-type: none"> • Availability, Inherent • Availability, Operational • Maximum time to repair (maxTTR) 	<ul style="list-style-type: none"> • Mean-time between downing events • Mean Time Between Failures (MTBF) • Mean Time To Repair (MTTR) • Mission Profile
<p>Maintainability related performance requirements for Built-in Test (BIT). Some specific potential requirements for BIT are listed below:</p> <ul style="list-style-type: none"> • mean time to fault isolate • percent maximum false alarm rate for BIT • Fault Isolation Capability for _____ percent of LRUs. • Percent fault detection through integrated diagnostics 	
<p>The probability of mission or mission phase success. R&M performance requirements must clearly define the success criteria for the mission or mission phase. Partial mission success probability requirements may also be specified in terms of sub-missions or particular scientific goals. The level of confidence associated with the probability value to be demonstrated should also be specified.</p>	
<p>Performance requirements dealing with probability of failure-free operation over a specified period of time. This requirement type is generally levied to a system or subsystem associated with the mission. The requirement must clearly define what constitutes a failure of the system or subsystem. The level of confidence associated with the probability value to be demonstrated should also be specified.</p>	
<p>Maintainability requirements such as Mean-Time To Repair (MTTR) and Maximum corrective maintenance time (for a certain percentile of failures) (MmaxCT at the XXth percentile). These R&M parameters provide the contractor adequate performance parameters needed for his design and verification effort as well. As with reliability, it may be necessary to specify different MTTR/MmaxCT requirements for different systems/subsystems.</p>	

content of many of the R&M activities and will directly impact the LCC efforts previously described. The operations concept, and its associated maintenance concept will also influence and subsequently be influenced by the initial logistics analyses that are also performed during Formulation. The logistics analyses like the LCC analyses depend heavily on R&M data to describe the operational profile of systems in terms of operational time and downtime related to failure and maintenance. As the design matures, the logistics analyses and the LCC analyses may identify changes that need to be made to the operations and maintenance concepts. Conversely, changes in the operations and maintenance concepts may require changes in the logistics and LCC analyses.

6.2.7 Developing a Fault Detection, Isolation and Recovery (FDIR) Capability

The main goal of fault detection, isolation, and recovery (FDIR) is to effectively detect faults and accurately isolate them to a failed component in the shortest time possible. Development and use of such a capability leads to reduction in diagnostic time or downtime in general and, therefore, increased system availability. A good inherent diagnostic of a system also enhances the crewmembers' confidence in operating the system, the main driver of mission success. Effective FDIR can keep a difficult to maintain system up and running where normal methods would lead to system downtime. FDIR is especially beneficial to an on-orbit system where maintenance may be impossible. The operations concept should contain provisions for developing effective FDIR for the operational portion of the life cycle.

6.3 Risk Management Activities Related to R&M

A fundamental element of Formulation is the initiation of program/project risk management activities. Early integration of risk management activities is essential to the long term success of the program/project in identifying and resolving the risks associated with the system. R&M processes, analyses and tasks are significant ingredients in the overall risk management process.

6.3.1 Preparing the Risk Management Plan (RMP)

The RMP is prepared during Formulation. The RMP, including appropriate R&M elements will be tailored to meet the specific program/project goals and structure.

The plan should be developed with the ultimate goal of providing the appropriate balance in risk acceptance and risk mitigation based on program/project objective and resource constraints. The Risk Management Plan provides process and organizational details of how the risk management effort will be accomplished and identifies the procedures, methods, tools and metrics to be used during the program/project. This will include the integration of any R&M related risk management activities such as the performance of Failure Modes and Effects Analyses, Reliability Predictions, Trade Studies, etc.

6.3.2 Establishing Mission Success Criteria

As previously discussed, Formulation is where the performance assessment criteria for the program/project are developed. Those performance assessment criteria related to mission success are important considerations in the risk management and R&M processes. These performance criteria establish the thresholds against which success or failure will be measured. A thorough

understanding of the relationship of mission needs to the system design is very important to establishing the R&M performance requirements and to making the final system or product reliable and maintainable. Knowledge of “how” the system design is evolving and the potential impacts on R&M performance requirements must be thoroughly understood. (Paragraph 6.2.4 discusses development of the R&M related performance and mission success criteria.)

6.3.3 Preliminary Risk Identification and Risk Mitigation Planning

As in the cases of LCC and logistics, Formulation is also when the initial risk assessments are performed. These initial assessments identify the risks associated with the program/project and start the process of mitigating those risks. The initial risk assessments also start to estimate the probability of occurrence and the associated uncertainty of those estimates. R&M analytical techniques are capable of providing some of this information and should be considered when developing the Risk Management Plan and when identifying the risks to the program/project. Besides initiating risk mitigation activities, such as redesigns or establishing risk controls, one important result of the initial identification efforts will be to establish program reserves for resolution of risks during the course of the program/project.

6.3.4 Capturing Risk History and Lessons Learned

While the focus of each program/project is to successfully meet its defined goals, there is a very important secondary consideration about documenting historical information for use in Formulation for other programs/projects. R&M lessons learned provide essential information for future programs/projects as well as for future generations of R&M or risk professionals. The Lessons Learned Information System (<http://llis.gsfc.nasa.gov/llis/llis.html>) and the R&M Best Practices (NASA Technical Memoranda 4322 and 4628 at <http://www.hq.nasa.gov/office/codeq/rmpro4a.htm>) provide a location to access and store this type of information.

CHAPTER 7 - R&M IN APPROVAL

7.1 Goal of Approval

The goal of Approval is to decide whether a program/project is ready to proceed from Formulation to Implementation. In a broad sense, Approval examines all of the results from Formulation and determines if the program/project is still consistent with NASA strategic objectives. In addition, it determines if the resulting plans and data from Formulation demonstrate that cost, schedule, and performance can be reasonably expected to be achieved for the remainder of the program/project. In actual practice, the decisions will focus on the content and scope of the Proposed Program Commitment Agreement and the Program/Project Plan as well as any significant information gathered during the performance of Non-Advocate Reviews or Independent Assessment activities conducted during Formulation.

7.2 Activities Related to R&M

There are no specific R&M activities that need to be performed during Approval. R&M's primary role in this process will be in supporting interpretation or explanation of any of the R&M information or data prepared or collected during Formulation.

CHAPTER 8 - R&M IN IMPLEMENTATION

8.1 Goal of Implementation

The goal of Implementation is to convert a set of performance requirements derived from Program Commitment Agreements into capable systems and/or technologies through which the mission needs are satisfied. During this conversion, early and continual R&M involvement should be used as detailed design is accomplished and hardware is constructed and operated.

8.2 Program/Project Management Activities Related to R&M

NPG 7120.5A describes the major activities that the program/project manager must accomplish during Implementation. R&M has a substantial role in the performance of many of these broad and varied activities that occur during Implementation. The following sections focus on the primary program/project management areas where R&M has a significant influence: requirements definition, systems design, test and verification, and operations and logistics.

8.2.1 Requirements Definition

8.2.1.1 Conversion of Program/Project Requirements into Specifications

Successful development of highly reliable and maintainable systems or products in Implementation requires translating the operational system requirements developed during Formulation into specific R&M and availability performance requirements that can be clearly defined, designed to, measured and verified. This section concentrates on defining and writing quantitative performance-based contract R&M requirements.

8.2.1.2 The Need for R&M Performance Requirements on NASA Programs/Projects

In the past, cost and litigation problems have risen on government contracts when the customer used specification requirements (such as Military-Specifications) to tell the manufacturer “how to” make the product. Often either an entire specification was invoked or a series of somewhat related specifications were invoked rather than being tailored to the specific procurement. This created a cost and schedule burden on the government in unnecessary requirements and testing. Today, the trend is to write system performance-based requirements into new NASA contracts as a means of motivating the supplier to incorporate workable and affordable requirements and solutions (including R&M) into the program/project. To accomplish this, the supplier must integrate R&M processes early in the system acquisition process, apportion the customer’s system performance-based R&M requirements down to the components and assemblies that combine to make the system, and demonstrate that the program/project, system, or product operational performance will meet the customer needs or goals. The central idea is paying for successful results, not just best efforts.

8.2.1.3 Defining R&M Performance Requirements

System specifications define the functional, performance, and interface requirements for the system or products. They establish a functional baseline and include a top-level description of the system or product architecture and operations. The system specifications provide the basis for establishing R&M performance requirements. To achieve compliance with the R&M program,

R&M performance requirements must be traceable to the overall program/project performance requirements for each item of hardware and software. The R&M performance requirements become the basis for quantitative and qualitative criteria for engineering design, system feasibility studies, failure mode identification, cost studies, trade-off decisions, and flight demonstration testing. Performance specifications also communicate the customer's requirements to the supplier. Incorporating R&M performance requirements as part of the system end item performance specification simply means writing specifications that will contain:

- precise definition of the equipment or system operational environment and mission profile(s);
- the system failure definition, including the minimum threshold of R&M performance requirements that will satisfy the customer's needs
- metrics that contain verifiable and unambiguous R&M performance requirements .

These R&M performance requirements will tell the supplier:

- what the customer will consider as an acceptable product or system
- how the customer will determine this acceptability.

A well written specification ensures that the customer understands what he will receive, and that the supplier understands what must be delivered to satisfy the R&M contract. **The most important thing to remember is to state R&M performance requirements in terms of the required results and provide the criteria for verifying compliance**, without stating the methods for achieving the results.

Quantitative reliability requirements provide specific design criteria for assuring that a system will meet its intended reliability and longevity. Early in the design process, the system developer needs to determine how the design will provide the requisite reliability characteristics that are needed for the delivered hardware and software to meet the program/project objectives and goals. Assessments of the design's ability to meet quantitative reliability requirements will support the design trade-offs, the component selection process, and the design for maintainability. These assessments will also determine appropriate levels and types of redundancy that are needed within the system to satisfy the R&M performance requirements.

It should be emphasized that use of quantitative performance-based reliability requirements does not supersede or negate the need for specifying fault tolerance or other classical reliability requirements. Fault tolerance requirements and reliability design criteria should also be levied to ensure the proper physical separation of redundancy and the avoidance of failure propagation. Quantitative requirements are levied to ensure that the operational performance and mission goals can be met with an accepted probability level or likelihood. In non-man-rated vehicles or systems, emphasis is on specifying a requirement that is sufficient to ensure a high likelihood of mission success, but not so high as to drive cost beyond reasonable bounds. The use of functional requirements and item redundancy for increasing the likelihood of mission success will likely be necessary to meet high quantitative reliability specifications; however, it should be noted that redundancy can add significant program/project costs, both in dollars and in launch weight and volume. Trade studies may be necessary to balance requirements for the likelihood of meeting a

mission objective against the reliability achieved with current manufacturing technologies and against various design options.

R&M parameters should use units of measurement related to: (1) operational readiness; (2) mission success; (3) maintenance manpower cost; and (4) logistics support cost. (Note: Many of the R&M parameters used in defining the overall program/project R&M performance requirements during Formulation can also be used in Implementation. The primary difference will be in the level of detail or indenture to which they are applied.) Typical reliability, availability, and maintainability parameters that are used to quantify R&M performance are described in Table 6-1. Appendices C and D identify sample text demonstrating various ways these parameters could be included in contract specifications used during Implementation.

Well-written R&M performance requirements support development of other program/project requirements such as safety, quality engineering, warranty, life-cycle costs (LCC), and logistics. Once these requirements are established, design guidelines can be prepared and submitted to the system designers. These design guidelines can be transformed and expanded through parametric analysis to derive cost estimations and cost-effectiveness trade-off relationships. The expanded design guidelines can be used further for validating/optimizing the R&M performance requirements. The R&M performance requirements that are being documented should take into account these guidelines to eliminate conflicts in program/project direction and inefficiencies in the application of engineering and management resources that will be used in achieving the R&M performance requirements.

8.2.1.4 Establishing R&M Incentives

Both monetary and non-monetary incentives can be used to access and measure contractor R&M performance. If properly formulated, R&M performance requirements stated in performance-based contracts, can ensure that the contractor or supplier will focus on the system or product R&M performance requirements of primary interest. This approach allows incentives to be awarded realistically based on the R&M performance measurements that are made during Implementation.

Two basic things must be taken into account when planning a monetary incentive program for obtaining a desired R&M response from contractors or suppliers.

- R&M performance requirements (i.e., testability or diagnostic) on which the incentives are based must be realistic, statistically sound, and unambiguous to permit valid demonstration/verification within realistic confidence bounds.
- The R&M incentive program should be adaptable and flow with the normal system development activities and schedules to minimize administrative costs and evaluation complexity

8.2.2 R&M Considerations in Systems Design

8.2.2.1 Typical/Example Considerations

Typical areas of design considerations for incorporating R&M in system design are shown in Table 8-1. The system developer prepares a team to perform the systems design and includes

some, or all, of these considerations and activities in their design process. The government oversees the performance of the design to assure that the completed design will meet the requirements specified.

Table 8-1. Considerations in Design for R&M

<ul style="list-style-type: none"> • Environmental stress screening (such as burn-in, temperature cycling and vibration testing) • FMEA • Reliability Centered Maintenance • Reliability Requirements • Redundancy • Parts selection criteria and control • Derating of parts • Reliability Plan • Components service • Conformal coating 	<ul style="list-style-type: none"> • Simplicity of design • Product survival in the intended mission environment (radiation, plasma, micro-meteor/orbital debris, humidity, temperature, mechanical shock, vibration, electromagnetic compatibility) • Predictions • Control of the physical environment • Expected operating and storage times (limited life items) • Failure propagation 	<ul style="list-style-type: none"> • Protection of cables, wires, receptacles, plug ends, connectors • Probabilistic Structural Analysis • Failure/fault tolerance • Use of preferred parts and materials • Verification of operational status for redundant paths • Redundancy management • Burn-in to eliminate infant mortality parts
---	--	---

The government's role could take many forms from being a member of the program/project team to performing assurance activities by monitoring progress based upon pre-established metrics. In any case, the government personnel monitoring the design process must have a thorough knowledge of the design requirements and understand how the developer is applying R&M techniques and analyses to assure that the design will perform adequately.

R&M engineers should perform selected R&M trade-off studies at the appropriate level, based on the complexity, and criticality of a design. Examples of such analyses that should be performed are listed in Table 8-2.

Table 8-2 R&M Trade-off Analysis Examples

<ul style="list-style-type: none"> • reliability prediction • R&M allocation • failure modes and effects analysis • criticality analyses 	<ul style="list-style-type: none"> • fault tree analysis • worst case circuit analysis • maintainability assessment.
--	---

If applied, the maintainability assessment should be not only an estimate of the mean-time-to-repair for various components of a system, but also a review of the components for crucial maintainability criteria such as those shown in Table 8-3.

Table 8-3 Critical Maintainability Criteria

<ul style="list-style-type: none">• Accessibility• interchangeability• failure detection• failure isolation	<ul style="list-style-type: none">• special tools and diagnostics• spares• logistics support sources
--	--

In addition, both the developer's R&M design activities and the government's R&M assurance activities should be closely integrated with related design activities particularly safety, human factors, software and logistics. A measure of the potential success of a program/project is the degree that all of these related design activities are integrated with each other. For example the review, analysis and resolution of hazard analyses (safety) as initiating events for R&M and/or human factors considerations provides an indication that the designers are working to provide a robust design.

8.2.2.2 Closed Loop Problem/Failure Reporting

As a tool for both the developer and the government, a closed loop problem/failure reporting and corrective action system should be established to support problem detection and assessment and hardware repair. This system will allow the developer to implement design improvements / corrections as part of the design process and provide the government with a tool for monitoring progress toward meeting the systems requirements. The data collected will support tracking the root cause of the problem and provide the basic data to be considered for addition to the NASA Lessons Learned Information System. The corrective action system should continue to be used in operations to support upgrading system R&M performance.

8.2.3 Test and Verification

8.2.3.1 R&M Performance Requirements Verification

Verification establishes that R&M performance requirements have been met. The customer, contractor/ supplier can use various verification techniques (e.g., test, analysis and inspection) to ensure that the system or product items being developed meet the R&M performance requirements and will perform effectively in the intended operational environment. An important factor to remember is that R&M performance requirements, which cannot be verified, are not considered valid requirements. Virtually all programs have some form of up-front planning which is usually captured in a set of documented program/project verification plans. As part of that set of documents, the contractor or supplier must prepare R&M test and evaluation plans which provide the details and the execution of the R&M performance and demonstration tests. It is essential that during R&M testing activities, adequate budgeting be provided for both the customer and the contractor to perform all the test programs necessary to verify the R&M performance requirements.

8.2.3.2 Test and Evaluation

Test and Evaluation (T&E) is a broad set of activities that includes the physical and analytic testing of components, subsystems, or systems during Formulation and Implementation. It includes testing during hardware and software integration and verification. R&M T&E is conducted to evaluate how well the system meets the specified R&M performance requirements. The continuous assessment approach for system T&E should provide feedback based on root cause analysis to improve the system design and R&M performance.

R&M performance requirements are the key inputs to the T&E process. R&M performance requirements normally result from the system engineering process and are documented in customer specification(s). Once the R&M performance requirements have been established and documented for the system, T&E can be planned in conjunction with the general planning and testing activities. Selection of the most appropriate verification method or methods for a given requirement should be based on the following:

- the test or evaluation method that can be applied by the contractor as early as possible in the system or product life-cycle to demonstrate compliance with the customer R&M performance requirements.
- the evaluation method or combination of methods or tests that are most effective for demonstrating R&M compliance with the system/product requirements, and
- the evaluation or test methods that are most efficient when considering the safety and cost risks involved.

Correct selection of a verification (i.e., T&E) method helps ensure that the end product(s) architecture remains in compliance with the R&M performance requirements as the program/project evolves. Verifying the R&M hardware performance requirements early in the program/project will provide timely logistics planning and spares projections; however, due to the early application it may not ensure that all R&M performance functions have been exercised. Effective T&E should balance the elements that are performed early in the design process to identify and correct problems with those elements that are performed later in the design process to verify that all system requirements have been met.

Typical types of testing and evaluation which may be essential for meeting system milestones and supporting successful system acquisition include the following:

- During early Implementation, investigate alternative designs through testing prior to selecting a final design.
- After construction has become mature, functional testing of subsystems and the integrated system will show that the system meets or approaches specifications.
- Environmental testing for certain types of equipment (as an example, off-gassing and out-gassing of equipment used in space habitats).
- Preliminary operational testing by the contractor prior to turnover and acceptance testing.

- In the operational phases after the customer has accepted the contracted system, both operational testing and system wearout and replacement testing by the evaluator to minimize costs to the customer.

A T&E plan should be tailored during Implementation for each contract such that it produces optimum results in verifying product acceptability. Examples of specific testing could be accelerated life tests during early Implementation to determine and predict an item's long term reliability or Extra-vehicular Activity maintenance testing in the Neutral Buoyancy Facility to determine the level of difficulty and amount of time needed to provide maintenance by an astronaut. The contractor should develop a matrix of all tests required to assure that the customer requirements are being met. From this matrix, the contractor will want to select only those tests that actually make economic and final product verification sense.

Early in Formulation, customer in-house testing may be necessary to identify whether a system concept is verifiable. Later in Formulation, the customer may test to develop acceptance criteria to be used in evaluating the contracted system. In either case, test data usually will have more fidelity than predictive data, consequently the data/results obtained from any of this testing can be used to improve the systems design as well as update preliminary information with data that more accurately reflects operational use. For example, failure rates used in LCC models could be updated to reflect operational data obtained during test. Some generic R&M T&E activities as related to the different program/project subprocesses are shown in Table 8-4.

Table 8-4 Typical R&M T&E Program/Project Process-Related Activities

R&M Testing and Evaluation	
Formulation	Implementation
<ul style="list-style-type: none"> • Concept Verification Testing • Testing for Acceptance Criteria 	<ul style="list-style-type: none"> • Alternative Design Testing • Functional Testing • Environmental Testing • Preliminary Operational Testing • Turnover & Acceptance Testing • System Wearout & Replacement Testing • Operational Testing • Maintainability Demonstration

Reliability analyses such as reliability block diagrams analysis are used to verify the fulfillment of quantitative requirements. The attribute of reliability, by definition, lies in the probabilistic realm while most performance attributes or parameters such as temperature, speed, thrust, voltage, or material strength contain more deterministic characteristics. Within the accuracy of the measuring devices, one can directly measure performance attributes in the deterministic realm to verify compliance with requirements. No such measuring device exists for probabilistic parameters like reliability. It is usually estimated through comparison with similar components or systems through inference, analysis, and the use of statistics. Table 8-5 shows an example of quantitative reliability requirements verification techniques.

A reliability requirement specified without a probability value, such as “the vehicle shall perform "xyz" mission on-orbit without failure for 5 years,” is impossible to verify during qualification or acceptance testing. The statistical likelihood, or probability, that the requirement will be met is assessable, and this activity is inherently equivalent to assessing the reliability. Without quantitative requirements, it is left to the certification assessor to evaluate an estimate of the probability of success and to decide if that is sufficient.

Table 8-5 Quantitative Reliability Requirements Verification Techniques

Verification Method	Program/Project Subprocess	Necessary Input
Reliability Analysis (Block Diagram Assessments, Availability Simulation)	Early Implementation	System architecture, system environment, mission time, appropriate component failure and repair data, etc.
Probabilistic Risk Assessment (Fault Tree Analysis, Event Tree Analysis)	Early Implementation	System architecture, test results.
Reliability Qualification or Acceptance Testing	Implementation.	Failure Data, test results, root cause analysis.

8.2.3.3 R&M System/Product Acceptance

As the final condition of R&M acceptance, the supplier/contractor needs to verify through appropriate demonstration or analyses that all the R&M functional and performance requirements have been met. Two configuration audits may be held in preparation for formal acceptance and turnover. These audits as identified below examine all of the resulting documentation from the design, development, test and evaluation activities to determine that the systems are completely and correctly documented and defined.

- **Physical Configuration Audit** - Conducted in accordance with established configuration management procedures to confirm that the physical characteristics of the system are accurately defined by the configuration documentation (specifications, drawings and software requirements and definition documents, etc.).
- **Functional Configuration Audit** - Conducted in accordance with established configuration management procedures to verify that the system performance has achieved the functional requirements specified in the configuration documentation (specifications, drawings, software requirements and definition documents, etc.).

8.2.4 Operations and Logistics

8.2.4.1 R&M during Operations

Operations is where the system will truly demonstrate its capability to meet the requirements developed during program/project Formulation. Operations also provides a unique opportunity to continue the evaluation and upgrading of the system(s) R&M performance with the dual benefit of

ensuring that the R&M performance meets and maintains intended capabilities and produces lower lifetime costs to the owner. The corrective action system developed during Formulation and Implementation should continue to be used in operations to support upgrading R&M performance.

Validation of hardware after operations have begun may be necessary to evaluate how the hardware is performing under actual operating conditions. History has shown typical reasons for such validation include: 1) flight hardware can be slightly different from qualification units; 2) environments may be significantly different from what was expected and qualified to, and 3) changes in subsystems can induce some surprises in performance characteristics.

Use of a structured and controlled data acquisition process provides the necessary information to perform trend analysis on the behavior of the subject equipment/project/program and to support root cause analyses of failure situations. As noted in Section 6.2.4, application of the R&M tools and techniques is extremely data-dependent and the root of oversight/insight into program/project behavior, validation decisions made earlier during Initiation, and identification of modifications/actions needed to sustain the program/project. For example, if Reliability Centered Maintenance were used during design early in Implementation, operations will provide the opportunity to validate or revise the maintenance decisions (redesign, condition monitor, hard-time task or run to failure) that were made during design. For the purpose of capturing lessons learned that can be used on future programs/projects, even one-shot system operation provides the capability to explore what did and did not go well. The most essential ingredient that will help guarantee the success of any operational R&M Program is management's continuing commitment and support.

8.2.4.2 Logistic Support

A logistic support concept is a statement of the general policy, ground rules and overall support approach for achieving the operational requirements. The concept in most cases is developed late in Formulation and describes the general approach to maintenance envisioned from the operational and mission requirements and from the maintenance ground rules. Used within the framework of an acquisition cycle for ground based systems, (a maintenance concept is not applicable for most unmanned flight hardware), the term relates to the general and tentative strategy during the Formulation and early Implementation subprocesses to govern design and the logistics planning effort with respect to allocation of maintenance tasks.

Logistics support considerations include concepts that are a composite of systematic actions taken to identify, define, analyze, quantify, and process logistics support needs. Table 8-6 illustrates typical contributing concepts. The program/project development team should identify the concepts appropriate to the system that system operators will use during mission support.

All aspects of logistics should be considered from spares to repairs. Development of Standard Maintenance and Repair procedures and programs should be part of Formulation and Implementation wherever appropriate for re-use of hardware to minimize operating costs in the operating phase. Often maintenance manuals are overlooked. Maintenance manuals should be developed for all levels of repair (in flight, on the ground at the NASA Center or at the suppliers plant). Manuals should also be validated to assure ease of accomplishing the work, feasibility, and safety (this validation could be performed as a part of the overall R&M T&E activities).

8.2.5 Risk Management Activities Related to R&M

The detailed portions of the risk management process will occur during Implementation. The Risk Management Plan will continue to evolve as the design and the program/project mature. For example, this could include the addition of participants in the risk evaluation process. The major emphasis in risk management during Implementation will be to identify the risks, assess their impact, prioritize them for mitigation/elimination and implement the mitigation/elimination actions. R&M will be a major participant in this process as many of the R&M tools, e.g., failure modes and effects analysis and reliability predictions, can be primary tools for the identification, quantification, and prioritization of risks. The structure of the program/project, the reviews to be performed and the schedules will dictate how R&M participates in the risk management process.

Table 8-6 Typical Logistics Support Considerations

<ul style="list-style-type: none"> • Maintenance concept • Maintenance analysis • System-level logistics support analyses • System design • Operational concept influence • Identification of supportability, cost, readiness drivers • Support concept development • Tradeoffs 	<ul style="list-style-type: none"> • Element-level logistics support analysis • Support system optimization • Resources requirements identification • Task and skill analysis • Early fielding analysis (to assess impact of introduction of the new system on existing systems) • Software logistics support for unmanned flight 	<ul style="list-style-type: none"> • Identification and correction of logistics problems • Postproduction support analysis • Supportability assessment plans and criteria • Support concept verification • Verification of resource requirements • On-board sparing /workarounds for unmanned flight
---	---	--

8.2.6 R&M Program/Project Reviews

One of the more important ways of controlling and evaluating the progress of a program is through forums and reviews. Each program/project should establish a series of reviews appropriate for the scope, duration and complexity of the program/project. The contractor may also establish similar internal reviews to assist in the control of the program/project. These reviews may take place during Formulation and Implementation; however, many of the more traditional reviews such as the Preliminary Design Review, Critical Design Review and Configuration Control Boards are performed during Implementation. Many of these reviews will also support Evaluation as described in Chapter 9.

There are basically two types of reviews that R&M will normally support; *technical* reviews and *decision point* reviews. Technical reviews are conducted by members of the technical teams and are normally scheduled to provide assistance in the resolution of complex technical issues, to

determine whether or not such issues exist, and for assistance in resolution of these same issues. Technical reviews can usually be accomplished without senior level personnel unless programmatic problems are identified. Some examples of NASA technical reviews are (1) engineering reviews, (2) audits, (3) Technical Interchange Meetings, (4) Interface Working Group meetings, and (5) program/project status reviews.

Decision point reviews are performed to determine if sufficient program/project progress has been made, the level of information that has been developed, and if enough of the requirements have been satisfied to begin performance of subsequent activities. Decision point reviews are normally held at critical points in the program/project to determine whether or not to continue and to validate at what funding and manpower levels the program/project should continue to operate. Decision point reviews normally require a mixed attendance including senior personnel and can encompass some or all elements of a technical review. Each program/project will define its own review structure. The following are examples of typical reviews where R&M is a consideration that might be included in a program/project.

Mission Concept Review (MCR) - The MCR is conducted during Formulation. The purpose of the MCR is to understand mission needs, and validate the proposed mission's objectives and concept for meeting those objectives.

System Requirements Review - The System Requirements Review is conducted during Formulation. The purpose of the System Requirements Review is to validate that the system requirements are fully developed and fulfill all mission needs.

System Definition Review - The System Definition Review is conducted near the completion of Formulation or the beginning of Implementation. Its purpose is to examine the proposed system architecture and the allocation of requirements to all functional elements of the system.

Preliminary Design Review (PDR) - The PDR is performed during Implementation. Its purpose is to demonstrate that the preliminary design meets all system requirements with acceptable risk. The PDR should also show that the correct design options have been selected, interfaces identified and defined with appropriate controls, and verification methodologies have been satisfactorily described. The PDR should also provide prerequisites for proceeding with detailed design.

Critical Design Review (CDR) - The CDR is conducted during Implementation. Its purpose is to disclose the complete system design in full detail, and ascertain that technical problems and design anomalies have been resolved without compromising system performance, reliability and safety. The CDR ensures that the design maturity justifies the program/project decision to initiate manufacturing, verification and integration of the mission hardware and software.

Test Readiness Review - The Test Readiness Review is conducted during Implementation. Its purpose is to ensure that appropriate test planning, facilities, personnel, plans and criteria are in place to proceed with the Test and Evaluation activities.

System Acceptance Review - The System Acceptance Review is held during Implementation near the end of system fabrication and integration stages and examines the

end items, documentation, test data and analyses that support verification. The R&M evaluator would ensure that the items have sufficient technical maturity to permit their transportation to and installation at the launch site or the operational ground facilities.

Flight Readiness Review (FRR) - The Flight Readiness Review is conducted during Implementation. Its purpose is to examine demonstrations, tests, analyses and audits which determine a system's readiness for safe and successful launch and subsequent flight operations. The R&M evaluator would ensure that all flight and ground hardware, software, personnel and procedures are operationally ready and compatible.

Operational Readiness Review - This review occurs during Implementation when the system is deemed ready for operation. The evaluator would examine all R&M system characteristics and operations to determine if the deployed state will fully support operations.

Decommissioning Review - The decommissioning review occurs when major items within a system or program/project are not needed. The R&M evaluator would be used to confirm that the reasons for decommissioning were valid and appropriate.

R&M should ensure that all pertinent R&M data necessary to support each review is provided in complete form and in a timely manner. This task includes all pertinent data on contractor and supplier-furnished articles (including Government Furnished Equipment) which are a part of the specific hardware/software assemblies to which the review pertains. In addition, R&M should ensure that adequate personnel are identified to participate in the reviews. As in other aspects of program/project development, the members of the R&M organizations should also be prepared to support the other disciplines that use or provide information related to R&M such as safety, logistics and human factors.

Generally after each review, the conductor of the review will document the results of the review including actions to be taken within a written report. All discrepancies found in the reviews should be quickly and successfully dispositioned. R&M should monitor the completion of those discrepancies or actions related to R&M.

One other forum that R&M typically participates in is the program/project configuration control board(s) (CCB). The CCB functions to manage changes to the requirements for the system as well as the design of the system. Depending on the size and complexity of the program/project there may be one board or several boards at different levels of design detail. During Implementation, particularly the design and operations portions of the subprocess, the design of the system changes as problems are resolved or improvements are identified. The CCB provides a formal process where each of these changes is documented and systematically evaluated to determine if they should be incorporated in the design. R&M plays an important part in this process since each change must be evaluated to determine if it increases, decreases or doesn't impact the R&M of the system.

CHAPTER 9 - R&M IN EVALUATION

9.1 Goal of Evaluation

The goal of Evaluation is to provide continuing assessments of the ability of the program/project to meet its technical and programmatic commitments and to provide value-added assistance to the program/project manager for successful completion of the program/project. As with Formulation, Approval and Implementation, R&M plays a significant role in Evaluation.

9.2 Evaluation Subprocess Activities Related to R&M

NPG 7120.5A stresses that Evaluation provides independent program/project assessments. These are in addition to the program/project internal reviews (e.g., System Requirements Review, Preliminary Design Review, Critical Design Review) described in paragraph 8.2.6. Evaluation monitors Formulation, Approval and Implementation to assure successful completion of the program/project. Evaluation uses independent R&M peers and the customers' R&M representatives to evaluate program/project performance and to identify technical achievements, issues and concerns as they relate to R&M. The R&M peers or customer representatives use their background, experiences, perspectives and lessons learned from other programs/projects to enhance the likelihood of success for the program/project being evaluated. The approved Program Commitment Agreement and/or the Program/Project Plan will specify the majority of these reviews; however, there may be circumstances when independent reviews are conducted based on external requirements such as Congressional request. While the scope of each of these reviews may vary, the themes of risk management, technical progress against the performance requirements and life cycle costs are common to all of these reviews.

As discussed in previous chapters, R&M can provide significant support in these three areas even if R&M performance is not a specific focus of the review. For example, R&M data support risk identification and mitigation, logistics analyses, system performance analyses and life cycle cost modeling. The reviews conducted during Evaluation also provide a unique opportunity to capture R&M lessons learned that can be documented for future use either in the NASA Lessons Learned Information System (<http://llis.gsfc.nasa.gov/llis/llis.html>) or the R&M Best Practices (NASA Technical Memoranda 4322 and 4628 (<http://www.hq.nasa.gov/office/codeq/rmpro4a.htm>).

APPENDIX - A R&M TOOLSETS

The following series of matrix-based R&M “Toolsets” provide brief descriptions of R&M-related analyses and activities that have proven effective on past programs. Each “tool” is accompanied by brief synopses of what the tool does, why it is used, when it is called for, and when during a program/project it is performed. In compliance with performance-based-contracting methodologies, these analysis techniques and activities are not to be specified in lieu of R&M performance requirements.

Note that the "tools are sorted in alphabetical order and not in the chronological order of their application or occurrence.

This appendix is provided for information only and should not be construed as a requirement or considered as an all-encompassing list. While contractors are at liberty to use any of the methods, they also are encouraged to develop and use their own R&M techniques.

Reliability Analysis Toolset

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	WHEN IT IS CALLED FOR	WHEN IT IS PERFORMED
Alert Reporting	Document significant problem and nonconforming item data for exchange among NASA Centers and GIDEP	Identifies potential problems	Used throughout a program / project (extends beyond just R&M)	As close to problem identification as possible
Approved Parts List	Identify parts to be approved for use on a given program/project.	Restricts use of parts to those meeting requirements.	Commonly used on spaceflight programs/projects.	Early in system design.
Human Error Risk Assessment	Identify risks to designs, equipment, procedures, and tasks as a result of human error.	Identifies candidate designs to support both risk and maintainability goals	For both ground and manned spaceflight programs/projects	Initially early in design and iteratively as the design matures
Human Factors Task Analysis	Analyze and list all the things people will do in a system, procedure, or operation with details on: (a) information requirements; (b) evaluations and decisions that must be made; (c) task times; (d) operator actions; and (e) environmental conditions.	Identifies influence factors that drive design for maintainability	For both ground and manned spaceflight programs/projects	Initially early in design and iteratively as the design matures
Deep Dielectric Charging & Internal ESD (IESD)	Conduct a materials inventory, resistivity analysis, and shielding assessment, and ascertain material susceptibility to deep dielectric charging and discharge.	Identifies the potential for a charged spacecraft conductor to cause an arc/pulse which can couple into the subsystem electronics.	For spacecraft to be subjected long-term to an energetic electron environment.	Potential IESD sources should be identified early in the program/project and eliminated.
Failure Mode and Effects (& Criticality) Analysis (FMEA/FMECA)	Perform a systematic analysis of the local and system effects of specific component failure modes. Under FMECA, also evaluate the mission criticality of each failure mode.	Identifies potential single failure points requiring corrective action. Identifies critical items and assesses system redundancy.	Should be considered even under a low cost mission regime.	When a system block diagram is available. Update throughout system design.
Fault Tree Analysis (FTA)	Systematically identify all possible causes leading to component failure or an undesirable event or state.	Permits systematic, top-down, penetration to significant failure mechanisms.	Apply to critical (especially safety-critical) mechanical & electromechanical hardware.	During system design.

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	WHEN IT IS CALLED FOR	WHEN IT IS PERFORMED
Ground Handling Analysis	Characterize the effects on equipment of ground handling and transportation.	Identifies potential problems related to handling effects, including temperature and humidity.	Where functional design of spacecraft structures must consider handling effects.	Early in design
Micro Meteoroid/ Debris Analysis	Predict the severity and frequency of particle collisions with a spacecraft under a specific mission profile.	Assesses spacecraft vulnerability to impacts.	When the system design suggests that impacts presents a risk to safety or the mission.	Early in design.
Parts Control Plan	Describes the process used to control the pedigree of component parts of a program/project	Provides a consistent means of identifying and controlling part lots, standardizing part selection, and controlling parts characteristics requirements	Appropriate for all hardware programs	Developed prior to parts selection and purchase
Parts Traceability	Trace parts pedigree from manufacturer to user	In the event of failure, provides a means to identify the source and production lot as well as to maintain consistency in parts control	Appropriate for all hardware programs	Early in design
Part Electrical Stress Analysis (PSA)	Subject each part to a worst-case part stress analysis at the anticipated part temperature experienced during the assembly qualification test.	Finds electrical and electro-mechanical piece parts that are electrically stressed beyond the limits imposed by the part derating criteria.	Nearly all spaceflight subsystems because PSA is cheap and eliminates potential single failure point parts.	During system design.
Physics of Failure Analysis	Identify and understand the physical processes and mechanisms which cause failure.	Minimizes the risk of failures by understanding the relationship between failure and driving parameters (environmental, manufacturing process, material defects).	For new product technology (e.g., electronic packaging, devices) or new usage of existing technology.	Throughout new technology development, and throughout the design and build processes.
Problem / Failure Reporting & Corrective Action System (PRACA / FRACAS)	Provide a closed loop system for documenting hardware and software anomalies, analyzing their impact on R&M, and tracking them to their resolution. (Root Cause Analysis)	Ensures that problems are systematically evaluated, reported, and corrected.	All programs/projects will benefit from some type of formal, closed loop system.	Throughout product acquisition and operations.

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	WHEN IT IS CALLED FOR	WHEN IT IS PERFORMED
Problem / Failure Reporting Plan	Document the process for closed-loop problem/failure identification, reporting, and resolution notification	Shows what problems exist within the program/project, what has been done to correct them, and the effectiveness of the remedial action.	At the outset of a program/project	Throughout product acquisition and operations.
Problem Avoidance Analysis	Review past problems (e.g., power on reset, circuit electrical noise susceptibility) to avoid a recurrence.	Reveals patterns of anomalous responses which may be indicative of major system problems.	As indicated by the failure history of the program/project.	Throughout product acquisition and operations.
Process Failure Modes and Effects Analysis	Analyze an operation / process to identify the kinds of errors that humans could make in carrying out the task.	A method to deduce the consequences for process failure and the probabilities of those consequences occurring.	To assist in control of critical processes.	Early in process definition
Radiation Dose Analysis	Assess the levels of ionizing dose and displacement damage that will occur inside the spacecraft.	Determine whether spacecraft shielding and radiation tolerance of electronics are sufficient to counter the cumulative effects of radiation.	Any spaceflight mission with a high radiation environment.	Early in design.
Redundancy Verification Analysis	Perform rigorous system-level modeling and analysis at the piece part-level for all redundant circuits.	Verifies that the failure of one of two redundant functions does not impair the use of the redundant path.	Particularly, for complex, long life systems featuring functionally redundant circuits.	During concept development.
Reliability Assurance Plan	Identify the activities essential in assuring reliability performance, including design, production, and product assurance activities.	Ensures that design risks are balanced against program/project constraints and objectives through a comprehensive effort calculated to contribute to system reliability over the mission life cycle.	For all programs/projects with reliability performance requirements.	During program/project planning.
Reliability Modeling (Prediction /Allocation)	Perform prediction, allocation, and modeling tasks to identify inherent reliability characteristics.	Aids in evaluating the reliability of competing designs.	Mainly for reusable or crewed systems, or where failure rates are needed for tradeoff studies, sparing analysis, etc.	Early in design.
Reliability Tradeoff Studies	Compare all realistic alternative reliability design approaches against cost, schedule, risk, and performance impacts.	Aids in deriving the optimal set of reliability performance requirements, architectures, baselines, or designs.	Conducted at some level on all systems. Predictive techniques may be used.	Formulation and Implementation.

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	WHEN IT IS CALLED FOR	WHEN IT IS PERFORMED
Single Event Effects (SEE) Analysis	Calculate the probability of device sensitivity to high-energy particle impacts in the anticipated environment, and minimize effects.	Prevent circuit failures caused by high-energy particle induced device upsets, latchups, gate ruptures, and transients.	For missions where device upsets are likely and can have serious consequences.	Early in design.
Sneak Circuit Analysis	Methodically identify sneak conditions (unexpected paths or logic flows) in circuits.	Identifies design weaknesses which could inhibit desired functions or initiate undesired functions.	Generally used only on the most safety or mission critical equipment.	Early in design.
Structural Stress Analysis	Analyze the dynamic stress to be experienced by mechanical/electro-mechanical subsystems/assemblies, including worst case estimates, for all anticipated environments.	Identifies spacecraft hardware issues related to stress on mechanical and electromechanical subsystems/assemblies, such as material fatigue.	When critical spacecraft assemblies are to be subjected to dynamic stresses.	During mechanical design.
Surface Charging/ESD Analysis	Analyze differential charging of nonconductive materials on the spacecraft surface to determine the energy that can be stored by each surface.	Identifies surfaces that are conceivable ESD sources and could cause unpredictable and catastrophic failures.	ESD should not be allowed to occur on surfaces near certain RF equipment nor on surfaces of solar arrays.	Early enough in the program/project so that effects can be mitigated by coatings, RC filters, alternate materials, etc.
Thermal Analysis of Electronic Assemblies to the Part Level	Calculate the temperature of all device failure sites (i.e., junctions, windings, etc.).	Identifies thermally overstressed parts, including excessive junction temperatures.	Whenever a Parts Stress Analysis is required.	Concurrently with the Parts Stress Analysis.
Thermal Stress/Fatigue Analysis	Analyze thermal effects on piece parts, assemblies, and subsystems, including worst case estimates, for all anticipated environments.	Addresses material fatigue and fracture, and the effect of thermal cycling on solder joints, conformal coating, and other critical materials.	When the design usage exceeds previously qualified temperature range and thermal cycling conditions.	Prior to or in conjunction with early design reviews.
Trend Analysis	Evaluates variation in data with the ultimate objective of forecasting future events based on examination of past results.	Provides a means of assessing the status of a program/project or the maturity of a system or equipment and to predict future performance.	Used to track Failures, anomalies, quality processes, delivery dates, etc.	Throughout the program/project

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	WHEN IT IS CALLED FOR	WHEN IT IS PERFORMED
Worst Case Analysis (WCA)	Evaluate circuit performance assuming part parameter variations associated with extreme conditions—long life, temperature, radiation, shock, etc.	Ensures that all circuits will perform within specifications over a given lifetime while experiencing the worst possible variations of electrical piece parts and environments.	Critical flight equipment.	During system design.

Maintainability Analysis Toolset

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	WHEN IT IS CALLED FOR	WHEN IT IS PERFORMED
Link Analysis	Arranges the physical layout of instrument panels, control panels, workstations, or work areas to meet specific objectives; e.g., increased accessibility.	Provides an assessment of the connection between (a) a person and a machine or part of a machine, (b) two persons, or (c) two parts of a machine	During design for maintainability	During Formulation and early Implementation
Logistics Support Analysis/Plan	Examine the resource elements of a proposed system to determine the required logistic support and to influence system design..	Provides an integrated and coordinated approach to meeting support requirements and attaining a maintainable design.	Where supportability and readiness are major concerns.	Early in concept development and design.
Maintainability Modeling (Prediction / Allocation)	Perform prediction, allocation, and modeling tasks to estimate the system mean-time-to-repair requirements.	Determines the potential of a given design for meeting system maintainability performance requirements.	Whenever maintainability requirements are designated in the design specification.	Early in design.
Maintenance Concept	Describe what, how, and where preventive and corrective maintenance is to be performed.	Establishes the overall approach to maintenance for meeting the operational requirements and the logistics and maintenance objectives.	Performed for ground and flight based systems where maintenance is a consideration.	During Formulation and revise throughout the life cycle.
Maintenance Engineering Analysis	Describe the planned general scheme for maintenance and support of an item in the operational environment.	Provides the basis for design, layout and packaging of the system and its test equipment and establishes the scope of maintenance resources required to maintain the system.	A Maintenance Plan may be substituted on smaller programs/projects where maintainability prediction and analysis is not a requirement.	Begins during design and is iterated through development.
Maintenance Plan	Describe in detail how the support program will be conducted to accomplish the program/project goals.	Identifies the desired long-term maintenance characteristics of the system, and the steps for attaining them.	Performed for ground and flight based systems where maintenance is a consideration.	Prepare during concept development and update throughout the life of the program/project.

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	WHEN IT IS CALLED FOR	WHEN IT IS PERFORMED
Reliability Centered Maintenance (RCM)	Determines the mix of reactive, preventive, and proactive maintenance practices to provide the required reliability at the minimum cost. Uses diagnostic tools and measurements to assess when a component is near failure and should be replaced	Minimizes or eliminates more costly unscheduled maintenance and minimizes preventive maintenance.	Called for as part of the Maintenance concept	During Implementation
Testability Analysis	Assess the inherent fault detection and failure isolation characteristics of the equipment.	Improves maintainability in response to operational requirements for quicker response time and increased accuracy.	Where maintenance resources will be available, but constrained.	Early in design.
Tradeoff Studies	Compare realistic alternative maintainability design approaches against cost, schedule, risk, and performance impacts.	Determines the preferred support system or maintenance approach in accordance with risk, performance, and readiness objectives.	Performed where alternate support approaches or maintenance concepts involve high risk variables.	Complete early in the acquisition cycle.

Reliability Test and Evaluation Toolset

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	WHEN IT IS CALLED FOR	WHEN IT IS PERFORMED
Acoustics Test	Subject potentially susceptible hardware to the dominant dynamic launch environment, with adequate margin.	Qualifies the design, and reveals design and workmanship inadequacies that might otherwise cause problems in flight.	For spacecraft structures with relatively large surface area-to-mass ratios, or for complete spacecraft.	At the earliest point the hardware is available for test.
Constant Acceleration Test	Subject equipment to high-G forces using a centrifuge.	Demonstrates the ability of spacecraft structures to withstand constant acceleration/deceleration.	Where hardware is to be subjected to high-G forces, especially upon landing.	During hardware qualification.
EMC Emissions Test	Test to identify unintentional radiated or conducted electromagnetic emissions from a system, subsystem, or assembly.	Qualifies flight hardware to launch vehicle requirements and assures that assemblies and subsystems will be electromagnetically compatible.	Used for assembly and system level compliance testing.	Prior to hardware integration at the next level of integration.
EMC Isolation Test	Measure the electrical isolation between power leads and structure, and between selected signal and command leads and structure.	Verifies that those circuits required to be isolated from the spacecraft structure to satisfy grounding s are in fact isolated.	Used for assembly and system level compliance testing.	Prior to hardware integration at the next level of integration.
EMC Susceptibility Test	Determine hardware susceptibility to electromagnetic radiation and to conducted ripple or transients on power and signal lines.	Verifies system hardness to the launch/boost/flight electromagnetic radiation environment, and radiated susceptibility safety margin for pyro devices.	Used for assembly and system level compliance testing.	Prior to hardware integration at the next level of integration.
Environmental Stress Screening	Subject parts to tests/environments that include burn-in, temperature cycling, and vibration.	Screens out parts subject to infant mortality.	Applies chiefly to high volume production.	Prior to assembly
ESD Discharge Test	Use electrostatic discharges to simulate the effects of arc discharges due to space charging.	Determines electromagnetic interference that may result when such discharges occur.	Missions where the environment may produce arcing due to differential charging.	During assembly level testing.
Ground Handling Test	Simulate the effects of ground handling and transportation dynamics.	Demonstrates the capability of equipment to withstand adverse handling conditions such as deteriorated highway road beds.	For critical non-flight hardware and for safety-critical flight hardware (e.g., explosive devices).	During hardware qualification.

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	WHEN IT IS CALLED FOR	WHEN IT IS PERFORMED
Highly Accelerated Life Test (HALT)	Conduct synergistic thermal, dynamic, and functional (voltage, clock margining) test-to-failure on prototype or surrogate hardware.	Rapidly identifies generic design, process, or workmanship problems in advance of the hardware build.	On new hardware technology or new processes, or to verify process stability.	Prior to hardware environmental test.
Highly Accelerated Stress Test (HAST)	Conduct synergistic thermal, dynamic, and functional (voltage, clock margining) accelerated stress screening.	Precipitates latent defects prior to product use.	On all high reliability flight hardware.	Prior to formal acceptance test.
Life Testing	Perform tests under conditions expected during life to determine the useful lifespan of the article under test.	Validates estimates of assembly lifespan.	Long missions/usage or unknown components.	Pre-PDR when flight-like surrogate hardware is available.
Magnetic Test	Measure DC magnetic fields that might be present due to materials or circuitry.	Verifies that the magnetic fields created by hardware are within acceptable ranges.	Driven by science complement or attitude control requirements.	During assembly level testing.
Mechanical Shock Test	Simulate dynamic effects due to sources other than pyrotechnic devices.	Qualifies the design for sources of shock such as pneumatic release devices and impact at the end of mechanical travel restraints.	Where mechanical shock (other than pyrotechnic) poses damage to flight equipment.	During hardware qualification.
Powered-On Vibration Test	Continuously monitor electrical functions while power is supplied to electronic assemblies during vibration, acoustics, and pyrotechnic shock.	Helps detect intermittent or incipient faults (arcing, open circuits, relay chatter) in electronic circuitry that may not be observed under ambient functional testing.	For equipment where intermittent or incipient failures could compromise essential functions.	Scheduled as part of a vibration test.
Pyrotechnic Shock Test	Simulate the dynamic effects resulting from the firing of pyrotechnic devices in spacecraft hardware, with adequate margin.	Qualifies the design, and demonstrates equipment survivability in a pyroshock environment.	Where the firing of pyros risks damage to flight equipment.	During both assembly-level hardware testing and system-level testing.
Random Vibration Test	Simulate the acoustically-induced vibration mechanically transmitted into hardware through attachments, with adequate margin.	Qualifies the design, and assists in finding existing and potential failures in flight hardware so that they can be rectified before launch.	For qualification and acceptance of spaceflight hardware subject to acoustically induced vibration.	At the earliest point the hardware is available for test.

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	WHEN IT IS CALLED FOR	WHEN IT IS PERFORMED
Reliability Demonstration	Conduct tests in a nonstressed environment to verify that the equipment meets functional and reliability performance requirements.	Verifies achievement of quantitative reliability and performance characteristics.	Only when expendable hardware is available, otherwise burn-in is conducted during system integration.	Following acceptance tests.
Reliability Growth Test	Conduct repetitive test and repair cycles to disclose deficiencies and verify that corrective actions will prevent recurrence.	Gradual evolution of a system to a state of higher reliability through repeated failure and repair.	For reusable equipment.	Beginning with design and throughout the product lifecycle.
Reliability Test Program Plan (Program/Project Specific)	Identifies and schedules tests used to assess and assure reliability throughout a the reliability program for a specific program/project	Controls resources and sequence of the overall reliability test program	For all programs/projects	Formulation, and Implementation
Root Cause Analysis	Identify the elemental cause(s) of reliability problems that could prevent recurrence of the problem	To reveal the true cause of a problem so that effective corrective action can be implemented	As problems/failures are identified	Formulation and Implementation.
Sine Dynamic (Sinusoidal Vibration) Test	Simulate the effects of mechanically transmitted, low-frequency launch vehicle transient events, with adequate margin.	Qualifies the design, and reveals failure modes not normally exposed by random vibration, and permits greater displacement excitation of the test item in the lower frequencies.	Useful where spacecraft structural integrity is an issue, assemblies were not qualified, or no structural proof loading test was conducted.	During hardware qualification.
Structural Proof Loading Test	Apply static forces to simulate worst case loading conditions, with adequate margin.	Demonstrates hardware design load capabilities.	For primary spacecraft structures.	When either a structural test model or a flight model is available for test.
Thermal Cycling Test	Simulate in a vacuum the effects of thermal cycling over unit life, with adequate margin.	Precipitates defects from design or manufacturing processes that could result in operational failure.	For assemblies that experience significant thermal cycling during their intended life, or that exceed the usage parameters to which they were previously qualified.	Prior to hardware integration at the next level of assembly.

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	WHEN IT IS CALLED FOR	WHEN IT IS PERFORMED
Thermal Shock Test	Subject mechanical, electronic, and spacecraft structural assemblies to a high rate of temperature change in a vacuum, with adequate margin.	Qualifies hardware for high ramp rates which could cause material fatigue or fracture due to thermal expansion.	Assemblies that experience wide ranges of temperature excursion with a high rate of temperature change (e.g., solar panels).	Prior to hardware integration at the next level of assembly.
Thermal Test	Simulate hardware design boundary conditions of conductive and radiative heat transfer, with adequate margin.	Qualifies hardware for vacuum and temperature conditions similar to the space environment. Screens for workmanship defects.	For critical hardware required to withstand significant deviations from ambient room temperature.	Prior to hardware integration at the next level of assembly.
Voltage / Temperature Margin Test	Exceed the expected flight limits of voltage, temperature, and frequency to simulate hardware worst case functional performance.	Permits real-time review of complex circuits, allowing the weighing of alternative design actions.	A viable alternative to Worst Case Analysis for flight programs/projects where tradeoffs of risk versus development time and cost are appropriate.	System design and integration.

Maintainability Test and Evaluation Toolset

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	WHEN IT IS CALLED FOR	WHEN IT IS PERFORMED
Maintainability Demonstration	Conduct formal simulations of equipment repair.	Verifies whether diagnostic/testability characteristics and quantitative maintainability characteristics meet system specifications.	For critical equipment where downtime must be minimized.	Prior to initial fielding of the system.
Root Cause Analysis	Identify the elemental cause(s) of maintainability problems that could prevent recurrence of the problem	To reveal the true cause of the problem so corrective action can be implemented.	As problems/failures are identified	During Formulation and Implementation.
Problem Failure Reporting	Provide a closed loop system for documenting hardware, software, and procedural anomalies impacting maintainability , analyzing their impact, and tracking them to their resolution. (Root Cause Analysis)	Ensures that problems are systematically evaluated, reported, and corrected.	All programs/projects will benefit from some type of formal, closed loop system.	Throughout product acquisition and operations. (Formulation through Implementation)
Reliability Centered Maintenance (RCM)	Determines the mix of reactive, preventive, and proactive maintenance practices to provide the required reliability at the minimum cost. Uses diagnostic tools and measurements to assess when a component is near failure and should be replaced	Minimizes or eliminates more costly unscheduled maintenance and minimizes preventive maintenance.	Called for as part of the Maintenance concept	During Implementation

Technical Review Toolset

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	WHEN IT IS CALLED FOR	WHEN IT IS PERFORMED
Detailed Technical Reviews	Conduct formal, informal, working-level, or peer reviews to assess interface compatibility and to prevent propagation of deficiencies to later products and to assure that the proposed design and implementation approach will satisfy the system and subsystem functional requirements..	Facilitates early detection and correction of design deficiencies. Provided for increased assurance that the proposed design approach, and the manufacturing and test implementation plans, will result in an acceptable product with minimal project risk.	As required to assess design compliance	.At various milestones as specified in the program/ project schedule and planning documents
Launch Readiness Review	Verify readiness to launch. Review risks associated with all unresolved problems.	Determines whether to permit the launch.	For all spaceflight payloads.	Prior to launch.
Monitor/Control of Suppliers	Provides confidence in integrity and pedigree of supplier products and services	Can establish long-term relationships with suppliers that enhance product reliability, quality, and repeatability.	As required to control design compliance	Formulation and early Implementation
Pre-Ship Review	Provide an independent assessment of product readiness for shipment.	Ensures the completeness and readiness of each item prior to release for shipment to another facility.	Where there is a need to review completion of development work before a product leaves the facility.	At the completion of the fabrication or build and testing of the item to be shipped.
Reliability Audits	Assess the effectiveness of subsystem/subcontractor reliability assurance activities.	Identifies necessary corrective actions to meet program/project R&M requirements.	Where required by the customer, or where subcontractor capabilities or the technology indicate possible problems.	Throughout design and development. Specific documentation may be required of the contractor at designated times.
Subsystem Inheritance Review	Review the design and test requirements and failure history of inherited hardware and designs.	Identifies risks associated with using inherited hardware in a new application.	When using inherited hardware.	Prior to subsystem technical reviews.

APPENDIX B

KEY R&M DISCIPLINE DEFINITIONS

Reliability Engineering

The objectives of this discipline are to define and support the implementation of the program/project reliability assurance plans such that the design risks are balanced with project objectives and constraints. This discipline performs reliability assessment and verification of the hardware design characteristics so that design deficiencies and functional performance risks are detected, accepted or mitigated early in the design process. Key activities within this discipline involve design architecture trade-offs, failure mode identification and problem avoidance, design analysis validation, functional performance validation with respect to operational environments and mission lifetime, integration of Human Factors concerns and issues, and technical evaluations of related programmatic risks. Early implementation of an adequate reliability assurance plan will benefit the program/project by contributing to a robust design, with an optimal balance between design verification tasks, cost, and schedule constraints, and minimize the probability of very late and costly detection of problems which could threaten mission launch schedules or mission objectives.

Environmental Requirements Engineering

The objectives of this discipline are to define the environmental design and verification requirements for the program/project based on the flight environment predictions. Identification and assessment of potential environment-driven failure mechanisms and the selection and use of analyses and tests capable of exposing and eliminating design/workmanship deficiencies related to these failure mechanisms is the foundation of this discipline. Key activities within this discipline consider the impacts of the program/project mission environments on design definition, verification (i.e., via analysis and test) and technical evaluations of related risks. Those activities benefit the program/project or task by increasing the confidence in the flight equipment capability to perform as required throughout exposure to the predicted mission environments. Environmental Requirements includes Dynamics, Thermal, Electromagnetic Compatibility and Natural Space Radiation and other space environments such as impacts of Micrometeoroids and Orbital Debris.

Problem/Failure Reporting

The objectives of this discipline are to define and support the implementation of an effective system for minimizing the probability of in-flight recurrence of problem and failure detected during the hardware and software development phase of the program/project. To avoid in-flight recurrences of functional nonconformance (including both actual and suspected problems/failures), Problem/Failure Reporting should be an integral part of a controlled, closed-loop system for problem/failure identification, reporting, analysis, and corrective action. This activity benefits the program/project by validating the adequacy and completeness of the investigation, analysis, and corrective action steps implemented to resolve hardware problems/ anomalies and will result in a high probability that in-flight mission threatening or mission catastrophic events will be avoided.

Electronic Parts Engineering

The Primary objective of the Electronic Parts Engineering is to assist the flight programs/projects in selecting and acquiring the best electronic parts for their applications within the constraints of their resources, risk tolerance, and schedule. This objective is met by (1) establishing guidelines for selection, procurement screening, and application of Electronic, Electrical, and Electro-mechanical parts, (2) reviewing performance relative to the program/project requirements, and (3) generating, maintaining, controlling Approved Parts Lists, as required. The benefits to the program/project include the best compromise of parts, functionality, characteristics, quality, and reliability that budgets and schedules can afford. An additional benefit is the insertion of new parts technology and, to the extent possible, the prevention of parts problems occurrence. The new small spacecraft and instruments must also make tradeoffs between existing parts and the use of customized parts to save mass and power. These are questions that are done within the Electronic Parts Engineering function.

Materials and Processes

The objectives of this discipline are to ensure that all materials and processes used in flight equipment are compatible with the mission requirements for structural integrity, functionality, outgassing, safety, etc. The activities encompass the selection and use of materials and processes. It develops, qualifies, evaluates and implements materials and process control requirements for the flight programs/projects. Materials and Processes benefit the program/project by ensuring efficient and cost effective use of materials and by ensuring the use of materials that are compatible with the mission requirements.

Maintainability Engineering

The objectives of this discipline are to define and support the implementation of the Program/Project Maintainability Assurance Plan and Maintenance Policy such that the operational risks are balanced with program/project objectives and constraints. This discipline performs maintainability assessments and verification of the system design characteristics so that the need for maintenance is minimized and downtime is minimized when maintenance action is necessary. Key activities within this discipline are design trade-offs, design for accessibility, design for ease of testing, manufacturing trade-off, testing trade-offs, operations trade-offs, evaluation of related programmatic risks, and performing Human Factors Analysis of the human-machine interface. Early implementation of an adequate maintainability assurance plan will benefit the program / project by contributing to an easy-to-use system, optimizing balance among design verification tasks, program/project tasks, schedule constraints, and minimizing the probability of very late and costly delays which could threaten mission success.

Mission Operations Assurance

Mission Operations Assurance function typically begins with the launch of the flight spacecraft / instrument, but may also begin as early as one year prior to launch, depending on the scope of preparation for launch and mission operations. The Mission Operations Assurance Functions identified below may be tailored to be consistent with the program/project risk tolerance. The

development and implementation of Mission Operations Assurance task focuses on robust processes and procedures, to reduce the risk of transmitting an incorrect command to the flight spacecraft/instrument. The thrust of the effort focuses on the prevention of errors in order to reduce the amount of resources required for rework and correction of command errors. These functions include:

- Uplink command assurance to reduce the risk of transmitting an incorrect command.
- Command and sequence uplink tracking to provide audit trail, reporting and trend analysis
- Coordination of command error tracking, investigation, correction and reporting
- Investigation, closure and tracking of in-flight hardware, software and operational anomalies
- Mission Operations process and procedure development and maintenance
- Risk management and reporting responsibilities to Program/Project and Safety and Mission Assurance
- Focus on adherence to processes and procedures and continuous process improvement

APPENDIX C

STATEMENT OF WORK - RELIABILITY AND AVAILABILITY

(NOTE: Not all possible requirements are listed, and not all listed requirements are necessarily applicable to all procurements. Italicized phrases are suggested modifications to be used in a Request for Proposal.)

1. The supplier shall describe how he will meet the reliability and availability requirements of the solicitation. If a supplier elects to submit a reliability and availability program plan, the plan will become a part of the contract upon contract award. In any event, the suppliers' responses will be evaluated using the following criteria.
 - 1.1. The supplier shall describe all activities considered to *{be necessary for ensuring the development of a}* have contributed to designing and manufacturing a reliable product. For each activity, the supplier shall describe the objective, rationale for selection, method of implementation, methods of assessing results, and any associated documentation.
 - 1.2 The supplier shall explicitly address how the included activities *{will be}* were integrated into the product and manufacturing design processes.
 - 1.3 The supplier shall show how the results of the included activities *{will be}* were used to support other activities, such as logistics planning, safety analyses, etc.
 - 1.4 The supplier shall explicitly show a clear understanding of:
 - the importance of designing-in reliability and availability
 - the relationship of reliability and availability to other system performance characteristics.
 - reliability and availability design techniques, methodologies, and concepts.
 - the importance of integrating reliability and availability activities into the overall systems engineering process.
 - a design reference mission profile used to establish adequate and complete R&M performance requirements.
 - 1.5 The supplier shall show how the following objectives *{will be}* were met:
 - feasibility of achieving required reliability and availability, including commercial and nondevelopment items.
 - identification of mission or safety critical single point failures and steps taken to avoid them.
 - demonstration that commercial and nondevelopment items will be operationally suitable for their intended use in the mission environment.
 - verification of requirements.

- evaluation of achieved reliability and availability, including commercial and nondevelopment items.

NOTE: For the next section, the reader is reminded that mandating tasks, even for new development, is somewhat risky because it relieves the suppliers of the responsibility for selecting the best means to accomplish the desired ends (in this case, meet the reliability and availability performance requirements). Mandating tasks should be done only after careful consideration of the advantages and disadvantages of doing so. Even then, suppliers should not be told how to accomplish the required task□

2. The following activities will be conducted by the supplier and reflected in the technical approach.
 - 2.1 Develop a reliability and availability model and make initial reliability and availability predictions using that model. All predictions shall be made at a stated level of confidence.
 - 2.2 Conduct a reliability and availability demonstration. The contractor shall explain how the demonstration will be implemented and the underlying statistical basis of the demonstration.
 - 2.3 Conduct dormant reliability analyses and an aging surveillance program for explosives, rocket motors, and other limited shelf-life items.
 - 2.4 Conduct part stress analyses and testing to verify compliance with derating criteria under worst-case mission profile environments.
 - 2.5 Implement a Failure Reporting, Analysis and Corrective Action System.
 - 2.x Conduct a _____ (NOTE: others as determined by buyer)
3. The supplier shall deliver the following reports and documents in accordance with the Contract Deliverables Requirements List (CDRL).

NOTE: User should enter all desired data items [reports, data, documents, etc.. Data items can include FMEA results, results of trade studies, BIT analyses results, and so forth. Data items should be selected based on the nature of the development, the level of risk, intended use of the item [benefit], and cost. The CDRL should provide due dates, any format requirements, etc.)

SPECIFICATION - RELIABILITY AND AVAILABILITY

(NOTE: Not all possible quantitative requirements are listed, and not all listed requirements are necessarily applicable to all procurements.)

1. The following levels of reliability and availability are required. Note: All values are the minimum acceptable values at a ____ confidence level, when appropriate.
 - 1.1 Platform-level (e.g., end product):
 - 1.1.1 ____ intrinsic/inherent availability
 - 1.1.2 ____ operational availability
 - 1.1.3 ____ mean time between failures (MTBF)
2. The product will be designed so that its reliability and availability will not be reduced due to the effects of being shipped by land, sea, or air or by periods of storage up to ____ .
(NOTE: User must state the storage period in either months or years.)
3. All reliability and availability requirements apply to the product as it will be used in the operating and support environment defined in Section _____ of the Specification and in accordance with the operating and support concepts defined in Section _____ of the _____.
4. Reliability and Availability must be satisfied without any maintenance action for single mission hardware. For reuse products maintenance shall not exceed ____% of End Item Cost over the life as specified in Section _____ of the end item specification.

APPENDIX D

STATEMENT OF WORK - MAINTAINABILITY

(NOTE: Not all possible requirements are listed, and not all listed requirements are necessarily applicable to all procurements. Italicized phrases are suggested modifications to be used in a Request for Proposal.)

1. The supplier shall describe how he will meet the maintainability performance requirements of the solicitation. If a supplier elects to submit a maintainability program plan, the plan will become a part of the contract upon contract award. In any event, supplier responses will be evaluated using the following criteria.
 - 1.1. The supplier shall describe all activities considered to *{be necessary for ensuring the development of a}* have contributed to designing and manufacturing a maintainable product. For each activity, the supplier shall describe the objective, rationale for selection, method of implementation, methods of assessing results, and any associated documentation.
 - 1.2 The supplier shall explicitly address how the included activities *{will be}* were integrated into the product and manufacturing design processes.
 - 1.3 The supplier shall show how the results of the included activities *{will be}* were used to support other activities, such as logistics planning, safety analyses, etc.
 - 1.4 The supplier shall explicitly show a clear understanding of:
 - the importance of designing-in maintainability and the relationship of maintainability to other system performance characteristics.
 - maintainability design techniques, methodologies, and concepts.
 - the importance of integrating maintainability activities into the overall systems engineering process.
 - the role of testability and diagnostics in maintainability and maintenance.
 - integrated diagnostics design principles.
 - 1.5 The supplier shall show how the following objectives *{will be}* were met:
 - design for accessibility.
 - design for human factors.
 - minimize number of special tools (design so faults can be readily and confidently detected and isolated).
 - design for testability.
 - design for ease of inspection and incorporate provisions for non-destructive inspection.
 - verification of requirements.

- evaluation of achieved maintainability.
- determine feasibility of achieving required maintainability.

NOTE: In using the next section, the reader is reminded that mandating tasks, even for new development, is somewhat risky because it relieves the suppliers of the responsibility for selecting the best means to accomplish the desired ends (in this case, meet the maintainability performance requirements). Mandating tasks should be done only after careful consideration of the advantages and disadvantages of doing so. Even then, suppliers should not be told how to accomplish the required task.

2. The following activities will be conducted by the supplier and reflected in the technical approach.
 - 2.1 Develop a maintainability model and make initial maintainability predictions using that model. All predictions shall be made at a stated level of confidence.
 - 2.2 Conduct an Integrated Diagnostics Analysis to identify the best mix of automatic, semi-automatic, built-in, and manual test capabilities; identify expected false alarm, cannot duplicate, and retest OK rates; and identify levels of isolation and ambiguity.
 - 2.3 Use computer modeling or other techniques to determine the accessibility of components for servicing and maintenance.
 - 2.4 Conduct an analysis, such as a Fault Tree Analysis or FMEA to assist in the efficient design of BIT and external test equipment and to assist in the identification of corrective maintenance requirements. Rationale for selecting the chosen analysis technique will be given.
 - 2.5 Conduct Human Factors analyses to ensure that any human-machine interface is acceptable.
 - 2.6 Conduct a maintainability demonstration. The contractor shall explain how the demonstration will be implemented and the underlying statistical basis of the demonstration
 - 2.7 Conduct a safety analysis to identify risks to support personnel.
 - 2.8 Conduct a _____ (NOTE: others as determined by buyer)
3. The supplier shall deliver the following reports and documents in accordance with the Contract Deliverables Requirements List (CDRL).

NOTE: User should enter all desired data items [reports, data, documents, etc.]. Data items can include FMEA results, results of trade studies, BIT analyses results, and so forth. Data items should be selected based on the nature of the development, the level of risk, intended use of the item [benefit], and cost. The CDRL should provide due dates, any format requirements, etc.

SPECIFICATION - MAINTAINABILITY

(NOTE: Not all possible quantitative requirements are listed, and not all listed requirements are necessarily applicable to all procurements.)

1. The following levels of maintainability are required. Note: All values are the minimum acceptable values at a ____ confidence level, when appropriate.
 - 1.1 Platform-level (e.g., end product):
 - 1.1.1 ____ mean time to repair
 - 1.1.2 ____ maximum active corrective maintenance time at the ____ percentile on a log-normal distribution
 - 1.1.3 ____ mean corrective maintenance time
 - 1.1.4 ____ mean preventive maintenance time
 - 1.1.5 ____ mean time to fault isolate
 - 1.1.6 ____ percent maximum False Alarm Rate for BIT
 - 1.1.7 ____ percent to ____ LRUs Fault Isolation Capability
 - 1.1.8 One hundred percent fault detection through integrated diagnostics
 - 1.1.9 ____ : average maintenance personnel skill level (customer-defined title or designation)
 - 1.2 Critical Systems (NOTE: User must define these)
 - 1.1.1 ____ mean time to repair
 - 1.1.2 ____ maximum active corrective maintenance time at the ____ percentile on a log-normal distribution
 - 1.1.3 ____ mean corrective maintenance time
 - 1.1.4 ____ mean preventive maintenance time
 - 1.1.5 ____ mean time to fault isolate
 - 1.1.6 ____ percent maximum False Alarm Rate for BIT
 - 1.1.7 ____ percent to ____ components or modules within LRUs Fault Isolation Capability
 - 1.1.8 100 percent fault detection through integrated diagnostics
2. The design of the product and all components shall be such that:
 - functionally different items cannot be interchanged
 - a fastener cannot be installed where a longer fastener is required

- equipment can be operated and maintained by personnel whose anthropometric dimensions are within the ____ percentile values for _____.

(NOTE: user must stipulate the percentile and whether it is for men, women, or both. Also, a reference from a military or other government or commercial standard giving the anthropometric measurements should be cited.)

- equipment can be operated and maintained by personnel wearing clothing appropriate for the range of climatic conditions described in Section _____.
- the probability of a catastrophic hazard to personnel during normal operation and maintenance is essentially zero.
- personnel do not have to lift or carry weights that exceed those prescribed for the ____ percentile _____.

(NOTE: user must stipulate the percentile and whether it is for men, women, or both. Also, a reference from a military or other government or commercial standard giving the maximum prescribed weights should be cited.)

3. The product will be designed so that its maintainability will not be reduced due to the effects of being shipped by land, sea, or air or by periods of storage up to _____ life units.

(NOTE: User must state the proper life units, either months or years.)

4. All maintainability requirements apply to the product as it will be used in the operating and support environment defined in Section _____ of the Specification and in accordance with the operating and support concepts